(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－242122
（P2003－242122A）
(43)公開日　平成15年８月29日(2003.8.29)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｃ　５Ｂ０８５
	３１０		３１０Ｄ

審査請求　未請求　請求項の数16　ＯＬ　（全 36 頁）

(21)出願番号　特願2002－41080(P2002－41080)

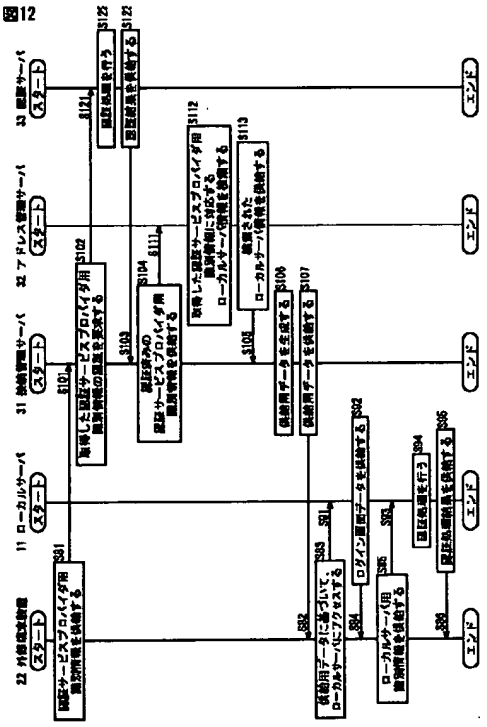
(22)出願日　平成14年２月19日(2002.2.19)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　後藤　和裕
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　黒岩　達雄
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　ネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラム

(57)【要約】
【課題】　より安全に通信を行う。
【解決手段】　外部端末装置は、ステップＳ８１において、認証サービスプロバイダの接続管理サーバにアクセスし、認証サービスプロバイダ用識別情報を供給する。接続管理サーバは、認証サーバに認証処理を行わせ、取得した認証サービスプロバイダ用識別情報に対応するローカルサーバ情報をアドレス管理サーバより取得し、接続管理サーバは、ステップＳ１０７において、取得したローカルサーバ情報に基づいて生成された、ローカルサーバのログイン画面のアドレス情報が含まれている供給用データを、外部端末装置に供給する。外部端末装置は、ステップＳ８３において、供給用データに基づいて、ローカルサーバにアクセスする。



【特許請求の範囲】

【請求項１】　ネットワークに接続され、他の情報処理装置と通信を行う第１の情報処理装置と、前記ネットワークに接続され、前記他の情報処理装置による、前記第１の情報処理装置への接続を管理する第２の情報処理装置とを備えるネットワークシステムであって、前記第１の情報処理装置は、前記他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定手段と、前記アドレス設定手段により設定された前記アドレスに関する情報を前記第２の情報処理装置に供給する第１の供給手段と、前記アドレスにアクセスした前記他の情報処理装置より供給される第１の識別情報の認証を行う第１の認証処理手段と、前記第1の認証処理手段による認証結果に基づいて、前記他の情報処理装置との接続を制御する接続制御手段とを備え、前記第２の情報処理装置は、前記第１の供給手段により供給された前記アドレスに関する情報を取得する第１の取得手段と、前記第１の取得手段により取得された前記アドレスに関する情報を記憶する記憶手段と、前記他の情報処理装置により供給される前記第１の情報処理装置への接続要求を受け付ける接続要求受け付け手段と、前記接続要求受付手段により受け付けられた前記接続要求の要求元である前記他の情報処理装置より第２の識別情報を取得する第２の取得手段と、前記第２の取得手段により取得された前記第２の識別情報の認証を行う第２の認証処理手段と、前記第２の認証処理手段により前記第２の識別情報が認証された前記他の情報処理装置に、前記第２の識別情報に対応する、前記記憶手段により記憶されている前記アドレスに関する情報を供給する第２の供給手段とを備えることを特徴とするネットワークシステム。

【請求項２】　ネットワークに接続され、第１の他の情報処理装置と通信を行う情報処理装置であって、前記第１の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定手段と、前記アドレス設定手段により設定された前記アドレスに関する情報を第２の他の情報処理装置に供給するアドレス情報供給手段と、前記アドレスにアクセスした前記第１の他の情報処理装置より供給される識別情報の認証を行う認証処理手段と、前記認証処理手段による認証結果に基づいて、前記第１の他の情報処理装置との接続を制御する接続制御手段とを備えることを特徴とする情報処理装置。

【請求項３】　前記アクセスを受け付けるアドレスは、前記情報処理装置に割り当てられたIPアドレスを含む基本アドレス、および、任意の文字列により構成される接続鍵を含み、前記アドレス設定手段は、前記基本アドレスを設定する基本アドレス設定手段と、前記接続鍵に関する設定を行う接続鍵設定手段とを備えることを特徴とする請求項２に記載の情報処理装置。

【請求項４】　前記接続鍵設定手段は、ユーザの指示に基づいて、前記ユーザにより入力された前記任意の文字列を用いて前記接続鍵を設定することを特徴とする請求項３に記載の情報処理装置。

【請求項５】　前記接続鍵設定手段は、任意の文字列を生成する文字列生成手段を備え、前記ユーザの指示に基づいて、前記文字列生成手段により生成された前記文字列を用いて、前記ユーザが指示する時間毎に、前記接続鍵を更新し、前記アドレス設定手段は、前記接続鍵設定手段により更新された前記接続鍵を用いて、前記アドレスに関する情報を更新し、前記アドレス情報供給手段は、前記アドレス設定手段により更新された、前記アドレスに関する情報を前記第２の他の情報処理装置に供給することを特徴とする請求項３に記載の情報処理装置。

【請求項６】　前記第２の他の情報処理装置に供給される認証鍵を取得する認証鍵取得手段と、前記認証鍵取得手段により取得された前記認証鍵を記憶する認証鍵記憶手段と、前記第２の他の情報処理装置に接続する際に、前記記憶手段により記憶されている前記認証鍵を前記第２の他の情報処理装置に供給する認証鍵供給手段とをさらに備え、前記認証鍵供給手段は、前記認証鍵取得手段により予め取得され、前記記憶手段により記憶されている前記認証鍵を前記第２の他の情報処理装置に供給し、前記アドレス情報供給手段は、前記認証鍵供給手段により供給された前記認証鍵に基づいて接続された前記第２の他の情報処理装置に、前記アドレスに関する情報を供給することを特徴とする請求項２に記載の情報処理装置。

【請求項７】　接続を許可するユーザの識別情報を記憶する識別情報記憶手段をさらに備え、前記認証処理手段は、前記識別情報記憶手段により記憶されている前記識別情報を用いて、前記第１の他の情報処理装置より供給された前記識別情報の認証を行うことを特徴とする請求項２に記載の情報処理装置。

【請求項８】　前記アドレスに関する情報を含む接続情報を前記第１の他の情報処理装置に供給する接続情報供給手段をさらに備えることを特徴とする請求項２に記載の情報処理装置。

【請求項９】　ネットワークに接続され、第１の他の情報処理装置と通信を行う情報処理装置の情報処理方法であって、前記第１の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、前記アドレス設定ステップの処理により設定された前記アドレスに関する情報の、第２の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、前記アドレスにアクセスした前記第１の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、前記認証処理ステップの処理による認証結果に基づいて、前記第１の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とする情報処理方法。

【請求項１０】　ネットワークに接続され、第１の他の

情報処理装置と通信を行う情報処理装置用のプログラムであって、前記第１の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、前記アドレス設定ステップの処理により設定された前記アドレスに関する情報の、第２の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、前記アドレスにアクセスした前記第１の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、前記認証処理ステップの処理による認証結果に基づいて、前記第１の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項１１】　ネットワークに接続され、第１の他の情報処理装置と通信を行う情報処理装置を制御するコンピュータが実行可能なプログラムであって、前記第１の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、前記アドレス設定ステップの処理により設定された前記アドレスに関する情報の、第２の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、前記アドレスにアクセスした前記第１の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、前記認証処理ステップの処理による認証結果に基づいて、前記第１の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とするプログラム。

【請求項１２】　ネットワークに接続され、第１の他の情報処理装置による、第２の他の情報処理装置への接続を管理する情報処理装置であって、前記第２の他の情報処理装置より供給されたアドレスに関する情報を取得するアドレス情報取得手段と、前記アドレス情報取得手段により取得された前記アドレスに関する情報を記憶するアドレス情報記憶手段と、前記第１の他の情報処理装置により供給された前記第２の他の情報処理装置への接続要求を受け付ける接続要求受け付け手段と、前記接続要求受け付け手段により受け付けられた前記接続要求の要求元である前記第１の他の情報処理装置から供給された識別情報を取得する識別情報取得手段と、前記識別情報取得手段により取得された前記識別情報の認証を行う識別情報認証処理手段と、前記識別情報認証処理手段により前記識別情報が認証された前記第１の他の情報処理装置に、前記識別情報に対応する、前記アドレス情報記憶手段により記憶されている前記アドレスに関する情報を供給するアドレス情報供給手段とを備えることを特徴とする情報処理装置。

【請求項１３】　認証鍵を生成する認証鍵生成手段と、前記認証鍵生成手段により生成された前記認証鍵を、前記第２の他の情報処理装置に供給する認証鍵供給手段と、前記認証鍵生成手段により生成された前記認証鍵を、前記認証鍵供給手段により前記認証鍵を供給した前記第２の他の情報処理装置に関する情報と関連付けて記憶する認証鍵記憶手段と、前記第２の他の情報処理装置より前記認証鍵を取得する認証鍵取得手段と、前記認証鍵記憶手段により記憶されている前記認証鍵を用いて、前記認証鍵取得手段により取得された前記認証鍵を認証する認証鍵認証手段と、前記認証鍵認証手段による認証結果に基づいて、前記第２の他の情報処理装置との接続を制御する接続制御手段とをさらに備え、前記アドレス情報取得手段は、前記接続制御手段による制御により接続された前記第２の他の情報処理装置から、前記アドレスに関する情報を取得することを特徴とする請求項１２に記載の情報処理装置。

【請求項１４】　ネットワークに接続され、第１の他の情報処理装置による、第２の他の情報処理装置への接続を管理する情報処理装置の情報処理方法であって、前記第２の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、前記アドレス情報取得制御ステップの処理により取得が制御された前記アドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、前記第１の他の情報処理装置により供給される前記第２の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、前記接続要求受け付けステップの処理により受け付けられた前記接続要求の要求元である前記第１の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、前記識別情報取得制御ステップの処理により取得が制御された前記識別情報の認証を行う識別情報認証処理ステップと、前記識別情報認証処理ステップの処理により前記識別情報が認証された前記第１の他の情報処理装置への、前記識別情報に対応する、前記アドレス情報記憶制御ステップの処理により前記記憶部からの出力が制御されている前記アドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とする情報処理方法。

【請求項１５】　ネットワークに接続され、第１の他の情報処理装置による、第２の他の情報処理装置への接続を管理する情報処理装置用のプログラムであって、前記第２の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、前記アドレス情報取得制御ステップの処理により取得が制御された前記アドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、前記第１の他の情報処理装置により供給される前記第２の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、前記接続要求受け付けステップの処理により受け付けられた前記接続要求の要求元である前記第１の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、前記識別情報取得制御ステップの処理により取得が制御された前記

識別情報の認証を行う識別情報認証処理ステップと、前記識別情報認証処理ステップの処理により前記識別情報が認証された前記第１の他の情報処理装置への、前記識別情報に対応する、前記アドレス情報記憶制御ステップの処理により前記記憶部からの出力が制御されている前記アドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項１６】　ネットワークに接続され、第１の他の情報処理装置による、第２の他の情報処理装置への接続を管理する情報処理装置を制御するコンピュータが実行可能なプログラムであって、前記第２の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、前記アドレス情報取得制御ステップの処理により取得が制御された前記アドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、前記第１の他の情報処理装置により供給される前記第２の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、前記接続要求受け付けステップの処理により受け付けられた前記接続要求の要求元である前記第１の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、前記識別情報取得制御ステップの処理により取得が制御された前記識別情報の認証を行う識別情報認証処理ステップと、前記識別情報認証処理ステップの処理により前記識別情報が認証された前記第１の他の情報処理装置への、前記識別情報に対応する、前記アドレス情報記憶制御ステップの処理により前記記憶部からの出力が制御されている前記アドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、ユーザ認証に用いられる識別情報を入力するための接続先アドレスを管理することによって、より安全に通信を行うことができるようにしたネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラムに関する。

【０００２】

【従来の技術】最近、インターネットの常時接続化やブロードバンド化とともに、家庭内等のローカルエリアにおいてもホームネットワークに代表されるLAN（Local Area Network）が普及してきている。ホームネットワークにおいては、通信機能を備えた家庭電化製品等が接続され、互いに情報を共有することができる。

【０００３】通信機能を備えた家庭電化製品としては、例えば、パーソナルコンピュータの他に、ビデオテープレコーダ等の画像録画再生装置、テレビジョン受像機、オーディオ機器、照明機器、空調機器、またはゲーム機等、様々なものが存在する。これにより、ユーザは、例えば、パーソナルコンピュータでビデオの予約をしたり、照明の点灯および消灯を制御したりすることができる。

【０００４】また、LANがインターネット等の外部のネットワークに接続されることで、LANに接続された機器同士で情報を共有するだけでなく、例えば、携帯電話機等からインターネットを介して、ホームネットワークに接続された家庭電化製品の動作を制御する等のように、外部の端末装置とも通信を行うことが可能になる。これによりユーザは、例えば、外出中であっても、携帯電話機を操作することで、自宅のパーソナルコンピュータが受信したメールを読んだり、テレビジョン放送の録画予約を行ったりすることができる。

【０００５】このとき、ホームネットワークに接続された家庭電化製品には、例えば、IPv6(Internet Protocol version 6)を用いて、それぞれグローバルなIPアドレスを割り当てておく。携帯電話機は、外部のネットワークおよびホームネットワークを介して、それらのIPアドレスを用いて、各機器と通信を行うことができる。

【０００６】しかしながら、この場合、家庭電化製品に割り当てられたIPアドレスが分かれば誰でも、外部のネットワークに接続された端末装置から、その家庭電化製品にアクセスすることができてしまう。

【０００７】これに対して、サーバ等により、外部のネットワークからのアクセスに対してユーザ認証を行い、特定のユーザからのアクセスのみを許可する方法がある。この場合、そのサーバは、HTML（HyperText Markup Language）等で記述されたWEBページを用いて、外部からアクセスしてきたユーザにID（IDentification）やパスワード等の識別情報を入力させ、その識別情報を予め登録されているユーザ情報に基づいて認証することにより、ユーザ認証を行う。すなわち、ユーザは識別情報を入力するWEBページのURL（Uniform Resource Locator）にアクセスし、識別情報をサーバに供給する。

【０００８】

【発明が解決しようとする課題】しかしながら、この場合、アクセス先のURLが固定されているため、セキュリティ上好ましくないという課題があった。例えば、許可されていない他のユーザでも、アクセス先のURLを知っていれば何度も識別情報の入力を試すことができるため、不正なログインを許可してしまう恐れがある。また、許可されていない他のユーザがアクセス可能な識別情報を入手した場合、その他のユーザは、サーバに登録されている情報を更新しない限り、容易に不正なログインを行うことができてしまう。

【０００９】また、ユーザが複数のLANに対してアクセス可能な識別情報を有する等して、接続先が複数存在す

る場合、それらの接続先のURLや識別情報等を全て管理することが困難な場合があるという課題があった。例えば、複数の接続先が存在するユーザは、その接続先の数だけURLや識別情報を、記憶したりメモをとったりするなどして管理し、適切に使用しなければならないので、非常に煩雑な作業を要する場合がある。

【００１０】本発明はこのような状況に鑑みてなされたものであり、より安全に通信を行うことができるようにするものである。

【００１１】

【課題を解決するための手段】本発明のネットワークシステムは、ネットワークに接続され、他の情報処理装置と通信を行う第１の情報処理装置と、ネットワークに接続され、他の情報処理装置による、第１の情報処理装置への接続を管理する第２の情報処理装置とを備えるネットワークシステムであって、第１の情報処理装置は、他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定手段と、アドレス設定手段により設定されたアドレスに関する情報を第２の情報処理装置に供給する第１の供給手段と、アドレスにアクセスした他の情報処理装置より供給される第１の識別情報の認証を行う第１の認証処理手段と、第１の認証処理手段による認証結果に基づいて、他の情報処理装置との接続を制御する接続制御手段とを備え、第２の情報処理装置は、第１の供給手段により供給されたアドレスに関する情報を取得する第１の取得手段と、第１の取得手段により取得されたアドレスに関する情報を記憶する記憶手段と、他の情報処理装置により供給される第１の情報処理装置への接続要求を受け付ける接続要求受け付け手段と、接続要求受付手段により受け付けられた接続要求の要求元である他の情報処理装置より第２の識別情報を取得する第２の取得手段と、第２の取得手段により取得された第２の識別情報の認証を行う第２の認証処理手段と、第２の認証処理手段により第２の識別情報が認証された他の情報処理装置に、第２の識別情報に対応する、記憶手段により記憶されているアドレスに関する情報を供給する第２の供給手段とを備えることを特徴とする。

【００１２】本発明の第１の情報処理装置は、第１の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定手段と、アドレス設定手段により設定されたアドレスに関する情報を第２の他の情報処理装置に供給するアドレス情報供給手段と、アドレスにアクセスした第１の他の情報処理装置より供給される識別情報の認証を行う認証処理手段と、認証処理手段による認証結果に基づいて、第１の他の情報処理装置との接続を制御する接続制御手段とを備えることを特徴とする。

【００１３】前記アクセスを受け付けるアドレスは、情報処理装置に割り当てられたIPアドレスを含む基本アドレス、および、任意の文字列により構成される接続鍵を含み、アドレス設定手段は、基本アドレスを設定する基本アドレス設定手段と、接続鍵に関する設定を行う接続鍵設定手段とを備えるようにすることができる。

【００１４】前記接続鍵設定手段は、ユーザの指示に基づいて、ユーザにより入力された任意の文字列を用いて接続鍵を設定するようにすることができる。

【００１５】前記接続鍵設定手段は、任意の文字列を生成する文字列生成手段を備え、ユーザの指示に基づいて、文字列生成手段により生成された文字列を用いて、ユーザが指示する時間毎に、接続鍵を更新し、アドレス設定手段は、接続鍵設定手段により更新された接続鍵を用いて、アドレスに関する情報を更新し、アドレス情報供給手段は、アドレス設定手段により更新された、アドレスに関する情報を第２の他の情報処理装置に供給するようにすることができる。

【００１６】前記第２の他の情報処理装置に供給される認証鍵を取得する認証鍵取得手段と、認証鍵取得手段により取得された認証鍵を記憶する認証鍵記憶手段と、第２の他の情報処理装置に接続する際に、記憶手段により記憶されている認証鍵を第２の他の情報処理装置に供給する認証鍵供給手段とをさらに備え、認証鍵供給手段は、認証鍵取得手段により予め取得され、記憶手段により記憶されている認証鍵を第２の他の情報処理装置に供給し、アドレス情報供給手段は、認証鍵供給手段により供給された認証鍵に基づいて接続された第２の他の情報処理装置に、アドレスに関する情報を供給するようにすることができる。

【００１７】接続を許可するユーザの識別情報を記憶する識別情報記憶手段をさらに備え、認証処理手段は、識別情報記憶手段により記憶されている識別情報を用いて、第１の他の情報処理装置より供給された識別情報の認証を行うようにすることができる。

【００１８】前記アドレスに関する情報を含む接続情報を第１の他の情報処理装置に供給する接続情報供給手段をさらに備えるようにすることができる。

【００１９】本発明の第１の情報処理方法は、第１の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、アドレス設定ステップの処理により設定されたアドレスに関する情報の、第２の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、アドレスにアクセスした第１の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、認証処理ステップの処理による認証結果に基づいて、第１の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とする。

【００２０】本発明の第１の記録媒体のプログラムは、第１の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、アドレス設定ステップの処理により設定されたアドレスに関する情報の、第２の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、アドレスにアクセスした

第１の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、認証処理ステップの処理による認証結果に基づいて、第１の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とする。

【００２１】本発明の第１のプログラムは、第１の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、アドレス設定ステップの処理により設定されたアドレスに関する情報の、第２の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、アドレスにアクセスした第１の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、認証処理ステップの処理による認証結果に基づいて、第１の他の情報処理装置との接続を制御する接続制御ステップとをコンピュータに実行させる。

【００２２】本発明の第２の情報処理装置は、第２の他の情報処理装置より供給されたアドレスに関する情報を取得するアドレス情報取得手段と、アドレス情報取得手段により取得されたアドレスに関する情報を記憶するアドレス情報記憶手段と、第１の他の情報処理装置により供給される第２の他の情報処理装置への接続要求を受け付ける接続要求受け付け手段と、接続要求受け付け手段により受け付けられた接続要求の要求元である第１の他の情報処理装置から供給された識別情報を取得する識別情報取得手段と、識別情報取得手段により取得された識別情報の認証を行う識別情報認証処理手段と、識別情報認証処理手段により識別情報が認証された第１の他の情報処理装置に、識別情報に対応する、アドレス情報記憶手段により記憶されているアドレスに関する情報を供給するアドレス情報供給手段とを備えることを特徴とする。

【００２３】認証鍵を生成する認証鍵生成手段と、認証鍵生成手段により生成された認証鍵を、第２の他の情報処理装置に供給する認証鍵供給手段と、認証鍵生成手段により生成された認証鍵を、認証鍵供給手段により認証鍵を供給した第２の他の情報処理装置に関する情報と関連付けて記憶する認証鍵記憶手段と、第２の他の情報処理装置より認証鍵を取得する認証鍵取得手段と、認証鍵記憶手段により記憶されている認証鍵を用いて、認証鍵取得手段により取得された認証鍵を認証する認証鍵認証手段と、認証鍵認証手段による認証結果に基づいて、第２の他の情報処理装置との接続を制御する接続制御手段とをさらに備え、アドレス情報取得手段は、接続制御手段による制御により接続された第２の他の情報処理装置から、アドレスに関する情報を取得するようにすることができる。

【００２４】本発明の第２の情報処理方法は、第２の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、アドレス情報取得制御ステップの処理により取得が制御されたアドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、第１の他の情報処理装置により供給される第２の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、接続要求受け付けステップの処理により受け付けられた接続要求の要求元である第１の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、識別情報取得制御ステップの処理により取得が制御された識別情報の認証を行う識別情報認証処理ステップと、識別情報認証処理ステップの処理により識別情報が認証された第１の他の情報処理装置への、識別情報に対応する、アドレス情報記憶制御ステップの処理により記憶部からの出力が制御されているアドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とする。

【００２５】本発明の第２の記録媒体のプログラムは、第２の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、アドレス情報取得制御ステップの処理により取得が制御されたアドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、第１の他の情報処理装置により供給される第２の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、接続要求受け付けステップの処理により受け付けられた接続要求の要求元である第１の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、識別情報取得制御ステップの処理により取得が制御された識別情報の認証を行う識別情報認証処理ステップと、識別情報認証処理ステップの処理により識別情報が認証された第１の他の情報処理装置への、識別情報に対応する、アドレス情報記憶制御ステップの処理により記憶部からの出力が制御されているアドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とする。

【００２６】本発明の第２のプログラムは、第２の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、アドレス情報取得制御ステップの処理により取得が制御されたアドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、第１の他の情報処理装置により供給される第２の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、接続要求受け付けステップの処理により受け付けられた接続要求の要求元である第１の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、識別情報取得制御ステップの処理により取得が制御された識別情報の認証を行う識別情報認証処理ステップと、識別情報認証処理ステップの処理により識別情報が認証された第１の他の情報処理装置への、識別情報に対応する、アドレス情報記憶制御ステップの処理により記

憶部からの出力が制御されているアドレスに関する情報の供給を制御するアドレス情報供給制御ステップとをコンピュータに実行させる。

【００２７】本発明のネットワークシステムにおいては、ネットワークに接続され、他の情報処理装置と通信を行う第１の情報処理装置と、ネットワークに接続され、他の情報処理装置による、第１の情報処理装置への接続を管理する第２の情報処理装置とが備えられ、第１の情報処理装置においては、他の情報処理装置からのアクセスを受け付けるアドレスが設定され、設定されたアドレスに関する情報が第２の情報処理装置に供給され、アドレスにアクセスした他の情報処理装置より供給される第１の識別情報の認証が行われ、その認証結果に基づいて、他の情報処理装置との接続が制御され、第２の情報処理装置においては、取得されたアドレスに関する情報が記憶され、受け付けられた他の情報処理装置からの第１の情報処理装置への接続要求の要求元である他の情報処理装置より第２の識別情報が取得され、その第２の識別情報の認証が行われ、認証された他の情報処理装置に、第２の識別情報に対応するアドレスに関する情報が供給される。

【００２８】本発明の第１の情報処理装置および方法、並びに第１のプログラムにおいては、第１の他の情報処理装置からのアクセスを受け付けるアドレスが設定され、設定されたアドレスに関する情報が第２の他の情報処理装置に供給され、アドレスにアクセスした第１の他の情報処理装置より供給される識別情報の認証が行われ、その認証結果に基づいて、第１の他の情報処理装置との接続が制御される。

【００２９】本発明の第２の情報処理装置および方法、並びに第２のプログラムにおいては、取得された第２の他の情報処理装置より供給されたアドレスに関する情報が記憶され、第１の他の情報処理装置により供給された第２の他の情報処理装置への接続要求が受け付けられ、その接続要求の要求元である第１の他の情報処理装置から供給された識別情報が取得され、取得された識別情報の認証が行われ、識別情報が認証された第１の他の情報処理装置に、識別情報に対応するアドレスに関する情報が供給される。

【００３０】

【発明の実施の形態】図１は本発明を適用したネットワークシステムの構成例を示す図である。

【００３１】建物などに代表されるローカルエリア１０に設置されたローカルサーバ１１は、ホームネットワーク等に代表される、ローカルエリア１０内のネットワークであるLAN１２に接続されている。また、ローカルエリア１０に設置された端末装置１３もLAN１２に接続されている。

【００３２】LAN１２は、図示せぬルータ等を介して、電話回線網やインターネット等に代表される、ローカルエリア１０の外部のネットワーク２１に常時接続されている。

【００３３】ローカルサーバ１１は、LAN１２を介して、例えば、端末装置１３等、ローカルエリア１０内に設置されているその他の機器の制御を行う。また、ローカルサーバ１１は、ローカルエリア１０の外部からのLAN１２への接続を許可するユーザに関する情報を有しており、ネットワーク２１から供給されたLAN１２への接続要求を取得し、ユーザ認証を行う。

【００３４】ネットワーク２１には、パーソナルコンピュータ等の外部端末装置２２が接続されており、外部端末装置２２は、ネットワーク２１を介してローカルサーバ１１と通信を行い、ローカルサーバ１１を制御したり、ローカルサーバ１１を介して、LAN１２に接続されている端末装置１３を制御したりすることができる。

【００３５】また、携帯電話機２３は、ネットワーク２１に接続された基地局２４と無線通信を行うことにより、ネットワーク２１と接続されており、この状態において、外部端末装置２２と同様に、ネットワーク２１を介してローカルサーバ１１と通信を行い、ローカルサーバ１１を制御したり、ローカルサーバ１１を介して、LAN１２に接続されている端末装置１３を制御したりすることができる。

【００３６】このとき、外部端末装置２２や携帯電話機２３は、ローカルサーバ１１にアクセスするために、ネットワーク２１を介して、認証サービスプロバイダ３０に設置されている接続管理サーバ３１と通信を行う。

【００３７】認証サービスプロバイダ３０は、ユーザ認証サービスを提供しており、ローカルエリア１０の外部からローカルサーバ１１へアクセスを行うユーザの認証処理を行う。

【００３８】認証サービスプロバイダ３０に設置されている接続管理サーバ３１は、ネットワーク２１に接続されており、ローカルエリア１０の外部からのLAN１２への接続要求を処理する。例えば、接続管理サーバ３１は、外部端末装置２２または携帯電話機２３からのローカルサーバ１１へのアクセスを管理する。

【００３９】また、認証サービスプロバイダ３０に設置されているアドレス管理サーバ３２は、ネットワーク２１を介してローカルサーバ１１より供給されたローカルサーバ１１に関する情報を管理する。また、アドレス管理サーバ３２は、接続管理サーバ３１にも接続されており、ローカルサーバ１１に関する情報を接続管理サーバ３１に供給することができる。

【００４０】認証サービスプロバイダ３０に設置されている認証サーバ３３は、アドレス管理サーバ３２に接続されており、認証サービスプロバイダ３０へのアクセスに対してユーザ認証処理を行う。例えば、ローカルサーバ１１がネットワーク２１を介してアドレス管理サーバ３２にアクセスした場合、認証サーバ３３は、ローカル

サーバ１１のユーザの認証処理を行う。また、例えば、外部端末装置２２がネットワーク２１を介して接続管理サーバ３１にアクセスした場合、認証サーバ３３は、アドレス管理サーバ３２を介して接続管理サーバ３１と通信を行い、外部端末装置２２のユーザの認証処理を行う。

【００４１】接続管理サーバ３１、アドレス管理サーバ３２、および認証サーバ３３は、認証サービスプロバイダ３０内において、互いに接続されているので、必要な情報を共有したり、処理を分散して実行させたりすることができる。

【００４２】図２は、図１に示すローカルサーバ１１の構成例を示すブロック図である。

【００４３】図２において、CPU（Central Processing Unit）５１は、ROM（Read Only Memory）５２に記憶されているプログラム、または記憶部６３からRAM（Random Access Memory）５３にロードされたプログラムに従って各種の処理を実行する。RAM５３にはまた、CPU５１が各種の処理を実行する上において必要なデータなども適宜記憶される。CPU５１、ROM５２、およびRAM５３は、バス５４を介して相互に接続されている。このバス５４にはまた、入出力インタフェース６０も接続されている。

【００４４】入出力インタフェース６０には、キーボード、マウスなどよりなる入力部６１、CRT（Cathode Ray Tube）、LCD（Liquid Crystal Display）などよりなるディスプレイ、並びにスピーカなどよりなる出力部６２、ハードディスクなどにより構成される記憶部６３、モデム、ターミナルアダプタ、またはLANアダプタなどにより構成される通信部６４が接続されている。

【００４５】記憶部６３には、ユーザに関する情報等を含むデータや、各種の処理を実行するためのプログラム等が記憶されており、CPU５１に制御され、RAM５３にデータやプログラムを供給する。

【００４６】通信部６４は、LAN１２を介しての通信処理を行う。例えば、通信部６４は、端末装置１３とLAN１２を介して通信を行ったり、ローカルエリア１０の外部の外部端末装置２２とネットワーク２１を介して通信を行ったりする。

【００４７】入出力インタフェース６０にはまた、必要に応じてドライブ７０が接続され、磁気ディスク７１、光ディスク７２、光磁気ディスク７３、或いは半導体メモリ７４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部６３にインストールされる。

【００４８】図３は、図１に示す外部端末装置２２の構成例を示すブロック図である。

【００４９】図３において、CPU１０１は、ROM１０２に記憶されているプログラム、または記憶部１１３からRAM１０３にロードされたプログラムに従って各種の処理を実行する。RAM１０３にはまた、CPU１０１が各種の処理を実行する上において必要なデータなども適宜記憶される。CPU１０１、ROM１０２、およびRAM１０３は、バス１０４を介して相互に接続されている。このバス１０４にはまた、入出力インタフェース１１０も接続されている。

【００５０】入出力インタフェース１１０には、キーボード、マウスなどよりなる入力部１１１、ディスプレイやスピーカなどよりなる出力部１１２、ハードディスクなどにより構成される記憶部１１３、モデム、ターミナルアダプタなどにより構成される通信部１１４が接続されている。

【００５１】記憶部１１３には、ローカルエリア１０のローカルサーバ１１にログインするのに必要なデータや、各種の処理を実行するためのプログラム等が記憶されており、CPU１１１に制御され、RAM１１３にデータやプログラムを供給する。

【００５２】通信部１１４は、ネットワーク２１を介しての通信処理を行う。例えば、通信部１１４は、ネットワーク２１を介して、接続管理サーバ３１やローカルサーバ１１と通信を行う。

【００５３】入出力インタフェース１１０にはまた、必要に応じてドライブ１２０が接続され、磁気ディスク１２１、光ディスク１２２、光磁気ディスク１２３、或いは半導体メモリ１２４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部１１３にインストールされる。

【００５４】図４は、図１に示す接続管理サーバ３１の構成例を示すブロック図である。

【００５５】図４において、CPU１５１は、ROM１５２に記憶されているプログラム、または記憶部１６３からRAM１５３にロードされたプログラムに従って、ローカルエリア１０の外部からのLAN１２への接続の管理に関する各種の処理を実行する。RAM１５３にはまた、CPU１５１が各種の処理を実行する上において必要なデータなども適宜記憶される。CPU１５１、ROM１５２、およびRAM１５３は、バス１５４を介して相互に接続されている。このバス１５４にはまた、入出力インタフェース１６０も接続されている。

【００５６】入出力インタフェース１６０には、キーボード、マウスなどよりなる入力部１６１、ディスプレイやスピーカなどよりなる出力部１６２、ハードディスクなどにより構成される記憶部１６３、モデム、ターミナルアダプタなどにより構成される通信部１６４が接続されている。

【００５７】記憶部１６３には、各種の処理を実行するためのプログラムやデータ等が記憶されており、CPU１５１に制御され、RAM１５３にデータやプログラムを供給する。

【００５８】通信部１５４は、例えば、ネットワークを

介して外部端末装置２２と通信処理を行う。また、通信部１５４は、アドレス管理サーバ３２と接続されており、アドレス管理サーバ３２と通信処理を行う。

【００５９】入出力インタフェース１６０にはまた、必要に応じてドライブ１７０が接続され、磁気ディスク１７１、光ディスク１７２、光磁気ディスク１７３、或いは半導体メモリ１７４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部１６３にインストールされる。

【００６０】図５は、図１に示すアドレス管理サーバ３２の構成例を示す図である。

【００６１】図５において、CPU２０１は、ROM２０２に記憶されているプログラム、または記憶部２１３からRAM２０３にロードされたプログラムに従って、ローカルサーバ１１のアドレス管理に関する各種の処理を実行する。RAM２０３にはまた、CPU２０１が各種の処理を実行する上において必要なデータなども適宜記憶される。CPU２０１、ROM２０２、およびRAM２０３は、バス２０４を介して相互に接続されている。このバス２０４にはまた、入出力インタフェース２１０も接続されている。

【００６２】入出力インタフェース２１０には、キーボード、マウスなどよりなる入力部２１１、ディスプレイやスピーカなどよりなる出力部２１２、ハードディスクなどにより構成される記憶部２１３、モデム、ターミナルアダプタなどにより構成される通信部２１４が接続されている。

【００６３】通信部２１４は、例えば、ネットワーク２１を介して、ローカルサーバ１１との通信処理を行う。また、通信部２１４は、接続管理サーバ３１および認証サーバ３３と接続されており、それらとの通信処理を行う。

【００６４】入出力インタフェース２１０にはまた、必要に応じてドライブ２２０が接続され、磁気ディスク２２１、光ディスク２２２、光磁気ディスク２２３、或いは半導体メモリ２２４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部２１３にインストールされる。

【００６５】次に動作を説明する。図１に示すネットワークシステムにおいて、LAN１２を管理するローカルサーバ１１のユーザ（図示せず）は、認証サービスプロバイダ３０の会員であり、認証サーバ３３にユーザ情報が登録されているとする。なお、ユーザがローカルサーバ１１購入時、またはセットアップ時に自動的に登録されるようにしてもよい。認証サーバ３３に登録されているローカルサーバ１１のユーザは、接続管理サーバ３１およびアドレス管理サーバ３２にログインするIDおよびパスワードからなる認証サービスプロバイダ用識別情報を有している。

【００６６】以上のようにして、認証サービスプロバイダ３０の会員であり、認証サービスプロバイダ用識別情報を有するユーザによりローカルサーバ１１が新たに設置されたり、または初期化されたりした場合、ローカルサーバ１１は、ネットワーク２１を介してアドレス管理サーバ３２に、ローカルサーバ１１に関する情報を供給し、ローカルサーバ１１を登録させる。

【００６７】図１に示すローカルサーバ１１によるローカルサーバ情報登録処理を、図６のフローチャートを参照して説明する。

【００６８】最初に、ステップＳ１において、ローカルサーバ１１のCPU５１は、初期化処理を行い、ローカルサーバ１１に関する情報であるローカルサーバ情報を生成する。

【００６９】ローカルサーバ情報には、機種情報、対応するユーザに関する情報、アドレス情報、およびアクセスに必要な接続キーに関する情報等を含んでいる。

【００７０】機種情報は、ローカルサーバ１１の機種名、製品番号、または性能に関する情報等を含み、ユーザに関する情報は、アドレス管理サーバ３２に接続した際に使用された認証サービスプロバイダ用識別情報や、その識別情報に対応する、既に登録されているユーザに関する情報等を含み、アドレス情報は、ローカルサーバ１１に割り当てられたアドレスまたは、ログイン画面の初期アドレス等の情報を含み、接続キーに関する情報は、接続キーおよびその設定に関する情報を含んでいる。

【００７１】次に、CPU５１は、通信部６４を制御して、認証サービスプロバイダ用識別情報を用いて、アドレス管理サーバ３２にアクセスする。そして、ステップＳ３において、アドレス管理サーバ３２より認証処理結果に関する情報を取得し、認証されたか否かを判定する。認証されたと判定した場合、CPU５１は、ステップＳ４に進む。

【００７２】ステップＳ４において、CPU５１は、ローカルサーバ情報をアドレス管理サーバ３２に供給し、サーバ用キーを要求する。サーバ用キーは、アドレス管理サーバ３２が生成し、ローカルサーバ１１に供給するキーであり、ローカルサーバ１１がアドレス管理サーバ３２にログインする際に使用される。

【００７３】後述するように、ローカルサーバ１１は、アドレス管理サーバ３２に定期的に接続する場合があり、その場合、ローカルサーバ１１は、認証サービスプロバイダ用識別情報を定期的にネットワーク３２に流してしまうことになり、セキュリティ上好ましくない。従って、ローカルサーバ１１が認証サービスプロバイダ用識別情報を用いてログインするのは、最初の１回だけにするようにする。すなわち、以降、ローカルサーバ１１がアドレス管理サーバ３２に再接続する際は、サーバ用キーを使用する。

【００７４】なお、サーバ用キーは認証サーバ３３に登録されているユーザ情報と関連付けて生成され、登録さ

れているので、ローカルサーバ１１が再び初期化されるまで有効である。

【００７５】アドレス管理サーバ３２にサーバ用キーを要求したCPU５１は、ステップＳ５に進み、サーバ用キーを取得したか否かを判定し、取得したと判定するまで待機する。なお、所定の時間が経過したり、エラーメッセージを取得したりした場合、CPU５１は、ローカルサーバ情報登録処理を終了する。

【００７６】サーバ用キーを取得したと判定した場合、CPU５１は、ステップＳ６に進み、取得したサーバ用キーを、例えば、記憶部６３に保存し、ローカルサーバ情報登録処理を終了する。

【００７７】また、ステップＳ３において、認証されていないと判定した場合、CPU５１は、ローカルサーバ情報登録処理を終了する。

【００７８】以上に説明したローカルサーバ１１によるローカルサーバ情報登録処理に対応して、アドレス管理サーバ３２は、ローカルサーバ情報登録処理を実行する。

【００７９】図１に示すアドレス管理サーバ３２によるローカルサーバ情報登録処理を、図７のフローチャートを参照して説明する。

【００８０】最初に、ステップＳ２１において、アドレス管理サーバ３２のCPU２０１は、ローカルサーバ１１より接続を要求されたか否かを判定し、要求されたと判定するまで待機する。

【００８１】ローカルサーバ１１が、図６のステップＳ２において、アドレス管理サーバ３２にアクセスし、接続を要求したと判定した場合、CPU２０１は、ステップＳ２２に進み、取得した認証サービスプロバイダ用識別情報に基づいて、認証処理を行う。CPU２０１は、通信部２１４を制御して、認証サーバ３３に取得した認証サービスプロバイダ用識別情報を供給し、ユーザ認証処理を実行させ、処理結果を取得する。

【００８２】そして、CPU２０１は、ステップＳ２３において、ローカルサーバ１１より取得した認証サービスプロバイダ用識別情報が認証されたか否かを判定する。認証されたと判定した場合、CPU２０１は、ステップＳ２４に進み、ローカルサーバ１１の接続要求を許可し、接続処理を行う。このとき、処理結果をローカルサーバ１１に供給する。ローカルサーバ１１のCPU５１は、供給された処理結果に基づいて、ステップＳ３において、認証されたか否かを判定する。

【００８３】そして、図７のステップＳ２５において、CPU２０１は、接続されたローカルサーバ１１より、ローカルサーバ情報を取得したか否かを判定し、取得したと判定するまで待機する。なお、所定の時間が経過したり、回線が電気的に切断されたり、エラーメッセージを取得したりした場合、CPU２０１は、ローカルサーバ情報登録処理を終了する。

【００８４】図６のステップＳ４において、ローカルサーバ１１により供給されたローカルサーバ情報を取得したと判定した場合、CPU２０１は、ステップＳ２６に進み、サーバ用キーを生成し、取得したローカルサーバ情報に関連付けて記憶部２１３に登録する。

【００８５】なお、サーバ用キーは、ローカルサーバ情報に関連付けて記憶されており、後述するように、サーバ用キーを用いたユーザ認証においては、サーバ用キーの認証とサーバ用キーを供給した装置の認証が行われる。従って、ローカルサーバ１１に割り当てられたサーバ用キーをその他の装置から使用することはできない。

【００８６】サーバ用キーを生成し、登録したCPU２０１は、ステップＳ２７において、通信部２１４を制御して、生成したサーバ用キーをローカルサーバ１１に供給し、ローカルサーバ情報登録処理を終了する。

【００８７】また、ステップＳ２３において、認証サーバ３３が認証サービスプロバイダ用識別情報の認証に失敗したと判定した場合、CPU２０１は、ステップＳ２８に進み、エラー処理を行い、ローカルサーバ情報登録処理を終了する。

【００８８】以上のようにして、ローカルサーバ１１が初期化されると、ローカルサーバ１１に関する情報からなるローカルサーバ情報がアドレス管理サーバ３２に供給され、登録される。

【００８９】以上のように登録されたローカルサーバ情報に含まれる接続キーに関する情報等により、後述するように、ログイン画面のアドレスが設定される。接続キーに関する情報は、ローカルサーバ１１において、ユーザにより入力される。

【００９０】図８は、ローカルサーバ１１における、ユーザが接続キーに関する設定を行う設定画面の様子の例を示す図である。

【００９１】図８において、設定画面２５１は、ユーザが接続キーに関する設定を入力するための画面であり、CPU５１等に制御され、出力部６２のディスプレイ等に表示されるGUI（Graphical User Interface）である。ユーザは、この設定画面２５１に基づいて、入力部６１のキーボードやマウス等を操作して、設定情報等を入力する。

【００９２】設定画面２５１においては、各種のタブが用意されており、ユーザがマウスを操作し、タブを選択することにより、様々な設定が行えるようになっている。図８においては、接続キータブ２５２が選択されており、接続キーに関する設定を行うことができるようになっている。

【００９３】設定画面２５１の中央部には、接続キー設定欄２５３が表示されており、ユーザが、接続キーを設定するか否か、接続キーを使用する場合、その内容を自動で変更するか否か等の設定を選択的に行うことができるようになっている。また、自動で変更する場合、その

時間間隔も設定できるようになっている。

【００９４】また、接続キー設定欄の下側には、接続キー入力欄２５４が設けられており、接続キー設定欄２５３において、接続キーの自動変更が行われないように設定されている場合、ユーザは、接続キー入力欄２５４に好みの接続キーを入力することができる。図８において、接続キー入力欄２５４には、文字列「04C3DAFA07234e3c94ECAC7800681515」が入力されている。

【００９５】図９は、ローカルサーバ１１における、ユーザが接続キーに関する設定を行う設定画面の様子の他の例を示す図である。

【００９６】図９において、ユーザは、設定画面２５１の状態タブ２６１が選択されており、接続キーに関するサービスの制御を行えるようになっている。

【００９７】設定画面２５１の状態タブ２６１の下には、接続キーに関するサービスの制御を行う、サービス制御設定欄２６２が設けられている。ユーザは、入力部６１を操作して、サービスを開始したり、停止したり、再起動したりすることができる。

【００９８】サービス制御設定欄２６２の下側には、ログイン画面のアドレス情報を表示するログイン画面URL表示欄２６３が設けられている。ログイン画面のURLは、基本のURLに接続キーを付加した構成となっている。すなわち、図９の場合、ログイン画面のURLは、基本のURL「http://00.11.222.3/aaa/bbb/ccc?」に接続キー「04C3DAFA07234e3c94ECAC7800681515」を付加された構成となっており、「http://00.11.222.3/aaa/bbb/ccc?LoginKey=04C3DAFA07234e3c94ECAC7800681515」と表示されている。なお、図９の場合、ログイン画面URL表示欄２６３には、通常のURLとSSL（（Secure Socket Layer））対応のURLが表示されている。

【００９９】SSLはインターネット等のネットワークで情報を暗号化して送受信するプロトコルであり、現在広く使われているWWW（World Wide Web）やFTP（File Transfer Protocol）などのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信するためのプロトコルである。SSLは公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことを目的としている。国際標準化機構により制定された、異機種間のデータ通信を実現するためのネットワーク構造の設計方針に基づき、コンピュータの持つべき通信機能を階層構造に分割したモデルであるOSI（Open Systems Interconnection）参照モデルではトランスポート層(第4層)にあたり、HTTP（HyperText Transfer Protocol）やFTPなどの上位のプロトコルを利用するアプリケーションソフトからは、特に意識することなく透過的に利用することができる。

【０１００】以上のように、ログイン画面のURLを構成することにより、例えば、接続キーを定期的に自動変更するように設定しておくことで、ログイン画面のURLは定期的に変更されるので、第３者がIDやパスワードを入手しても、認証サービスプロバイダ用識別情報を取得していないとログイン画面を開くことができないため、不正なアクセスを抑制することができる。

【０１０１】ローカルサーバ１１のユーザは、入力部６１のキーボードやマウス等を操作して、出力部６２のディスプレイ等に表示されている設定画面２５１に備えられているタブの中から、図８に示すように、接続キータブ２５２を選択し、接続キー設定欄２５３において、接続キーを使用するか否か、使用する場合は、接続キーを自動で変更するか否か、自動で変更する場合は、その変更を行う時間間隔を設定する。また、自動で変更しないと設定した場合、ユーザは、接続キー入力欄２５４に接続キーを入力する。なお、接続キーは、その文字数が制限されていてもよく、例えば１２８bitの３２文字までの文字列または数字列などにより構成されるようにしてもよい。

【０１０２】図８に示す設定画面２５１の入力が完了したユーザは、次に、入力部６１のキーボードやマウス等を操作して、状態タブ２６１を選択し、サービス制御設定欄２６２において、設定した接続キーのサービスを開始させる。なお、設定された接続キーおよびログイン画面のアドレス情報は、ログイン画面URL表示欄に表示される。

【０１０３】以上のように、ローカルサーバ１１において、接続キーはユーザにより設定され、有効化される。有効化された接続キーは、ローカルサーバ情報に含められ、アドレス管理サーバ３２に供給される。

【０１０４】以上のような接続キーに関する設定は、同様の操作を行うことで、いつでも更新することができる。そして、接続キーに関する設定が更新された場合、アドレス管理サーバ３２に登録されているローカルサーバ情報も更新される。この更新処理は、ユーザの指示により、または、自動で定期的に行われる。

【０１０５】図１に示すローカルサーバ１１によるローカルサーバ情報更新処理を、図１０のフローチャートを参照して説明する。

【０１０６】最初に、ステップＳ４１において、ローカルサーバ１１のCPU５１は、更新された接続キーをアドレス情報に付加し、記憶部６３に記憶されているローカルサーバ情報を更新する。

【０１０７】そして、ステップＳ４２において、CPU５１は、更新したローカルサーバ情報に記憶部６３に記憶しているサーバ用キーを付加し、通信部６４を制御して、ネットワーク２１を介してアドレス管理サーバ３２に供給する。ローカルサーバ情報を供給したCPU５１は、ステップＳ４３に進み、アドレス管理サーバ３２より、処理結果情報を取得したか否かを判定し、取得したと判定するまで待機する。なお、所定の時間が経過した

場合、CPU５１は、ローカルサーバ情報更新処理を終了する。

【０１０８】処理結果情報を取得したと判定した場合、CPU５１は、ステップＳ４４に進み、取得した処理結果情報に基づいて、処理結果を出力部６２のディスプレイ等に表示し、ローカルサーバ情報更新処理を終了する。

【０１０９】以上に説明したローカルサーバ１１によるローカルサーバ情報更新処理に対応して、アドレス管理サーバ３２もローカルサーバ情報更新処理を実行する。

【０１１０】図１に示すアドレス管理サーバ３２によるローカルサーバ情報更新処理を、図１１のフローチャートを参照して説明する。

【０１１１】アドレス管理サーバ３２のCPU２０１は、ステップＳ６１において、ローカルサーバ１１が図１０のステップＳ４２において供給したローカルサーバ情報およびサーバ用キーを、ネットワーク２１を介して取得したか否かを判定し、取得したと判定するまで待機する。

【０１１２】ローカルサーバ１１よりローカルサーバ情報およびサーバ用キーを取得したと判定した場合、CPU２０１は、ステップＳ６２に進み、新たに取得したサーバ用キーを記憶部２１３に登録済みのサーバ用キーと比較し、認証処理を行う。なお、このとき、サーバ用キーの認証だけでなく、例えば、ローカルサーバ情報の内容からユーザ認証やローカルサーバ１１の認証などを行うようにしてもよい。このように、複数の認証を行うことで、セキュリティをさらに向上させることができる。

【０１１３】認証処理が終了したCPU２０１は、ステップＳ６３において、ユーザが認証されたか否かを判定する。そして、認証されたと判定した場合、CPU２０１は、ステップＳ６４において、取得したアドレス情報に基づいて、記憶部２１３に登録されているローカルサーバ情報を更新する。

【０１１４】そして、ステップＳ６５において、CPU２０１は、処理結果情報を作成し、ネットワーク２１を介して、ローカルサーバ１１に供給し、ローカルサーバ情報更新処理を終了する。

【０１１５】また、ステップＳ６３において、認証に失敗し、認証されていないと判定した場合、CPU２０１は、ステップＳ６５に進み、処理結果情報を生成し、ローカルサーバ１１に供給し、ローカルサーバ情報更新処理を終了する。

【０１１６】以上のようにして、ローカルサーバ情報更新処理が行われるので、接続キーを自動的に変更するように設定した場合においても、認証サービスプロバイダ用識別情報をネットワーク２１に定期的に流出することを防止することができる。

【０１１７】次に、以上のように設定された接続キーを用いて、ローカルエリア１０の外部よりネットワーク２１を介してローカルサーバ１１に接続する方法について説明する。

【０１１８】外部端末装置２２からネットワーク２１を介してローカルサーバ１１にログインする場合について、図１２のタイミングチャートを参照して説明する。また、必要に応じて、図１３乃至図１６を参照して説明する。なお、外部端末装置２２のユーザは、ローカルサーバ１１に登録されており、IDおよびパスワード等からなる識別情報を有している。

【０１１９】最初に、外部端末装置２２のCPU１０１は、ステップＳ８１において、通信部１１４を制御して、ネットワーク２１を介して認証サービスプロバイダ３０の接続管理サーバ３１にアクセスし、認証サービスプロバイダ用識別情報を供給する。

【０１２０】図１３は、外部端末装置２２が接続管理サーバ３１にアクセスした際に、出力部１１２のディスプレイに表示されたWEBブラウザのログイン画面の例を示す図である。

【０１２１】図１３において、ログイン画面２８１には、IDを入力するID入力欄２８２、パスワードを入力するわ巣ワード入力欄２８３、ユーザが、入力部１１１のマウス等で操作することによりログインを指示するログインボタン２８４が表示されている。

【０１２２】ユーザが接続管理サーバ３１の所定のアドレスにアクセスすると、接続管理サーバ３１は、ネットワーク２１を介して、図１３に示すようなGUI情報を外部端末装置２２に供給する。外部端末装置２２は、そのGUI情報を取得すると、ディスプレイに表示されているWEBブラウザに図１３に示すようなログイン画面２８１を表示させる。

【０１２３】外部端末装置２２のユーザは、ID入力欄２８２およびパスワード入力欄２８３に、認証サービスプロバイダ用識別情報に含まれるIDおよびパスワードをそれぞれ入力し、マウス等でログインボタンを操作する。外部端末装置２２のCPU１０１は、ユーザによりログインボタン２８４が操作されると、入力されたIDおよびパスワードを、ネットワーク２１を介して、接続管理サーバ３１に供給する。

【０１２４】接続管理サーバ３１のCPU１５１は、ステップＳ１０１において、供給された認証サービスプロバイダ用識別情報を取得する。そして、ステップＳ１０２において、CPU１５１は、認証サーバ３３に、取得した認証サービスプロバイダ用識別情報を供給し、その認証を要求する。

【０１２５】図示せぬ認証サーバ３３のCPUは、ステップＳ１２１において、供給された認証サービスプロバイダ用識別情報を取得すると、ステップＳ１２２において、その識別情報に対して認証処理を行う。そして、認証サーバ３３のCPUは、ステップＳ１２３において、その認証結果を接続管理サーバ３１に供給する。

【０１２６】接続管理サーバ３１のCPU１５１は、ステ

ップＳ１０３において、通信部１６４を制御し、認証サーバ３３より供給された認証結果を取得し、認証されたと判定すると、ステップＳ１０４において、認証済みの認証サービスプロバイダ用識別情報を、アドレス管理サーバ３２に供給する。

【０１２７】ステップＳ１１１において、アドレス管理サーバ３２のCPU２０１は、通信部２１４を制御して、供給された認証済み認証サービスプロバイダ用識別情報を取得すると、ステップＳ１１２において、記憶部２１３に登録されている、取得した認証サービスプロバイダ用識別情報に対応するローカルサーバ情報を検索する。

【０１２８】そして、CPU２０１は、ステップＳ１１３において、通信部２１４を制御して、検索されたローカルサーバ情報を、接続管理サーバ３１に供給する。接続管理サーバ３１のCPU１５１は、ステップＳ１０５において、通信部１６４を制御して、供給されたローカルサーバ情報を取得する。

【０１２９】ローカルサーバ情報を取得した接続管理サーバ３１のCPU１５１は、ステップＳ１０６において、取得したローカルサーバ情報に基づいて、外部端末装置２２に供給するための供給用データを生成する。供給用データには、外部端末装置２２が供給した認証サービスプロバイダ用識別情報に対応するローカルサーバ１１のログイン画面のアドレス情報が含まれている。このとき、識別情報に対応するログイン画面のアドレス情報が複数存在する場合、供給用データには、複数のアドレス情報が含まれる。

【０１３０】供給用データを生成した接続管理サーバ３１のCPU１５１は、ステップＳ１０７において、通信部１６４を制御し、ネットワーク２１を介して外部端末装置２２に供給用データを供給する。

【０１３１】外部端末装置２２のCPU１０１は、ステップＳ８２において、通信部１１４を制御して、供給用データを取得すると、供給用データに基づいて、図１４に示すような、接続先であるローカルサーバの一覧を、出力部１１２のディスプレイに表示されるWEBブラウザに表示させる。

【０１３２】図１４は、WEBブラウザに表示されたローカルサーバ一覧画面の例を示す図である。

【０１３３】図１４において、ローカルサーバ一覧画面２９１の中央には、外部端末装置２２のユーザに対応してアドレス管理サーバ３２に登録されているローカルサーバであるパーソナルコンピュータ（以下、PCと称する）の一覧を表示するローカルサーバ一覧表示欄２９２が設けられている。外部端末装置２２のユーザが表示されているPCの中から目的のPCを選択し、マウス等でローカルサーバ一覧表示欄２９２内に表示されているアクセスボタン２９３を操作すると、CPU１０１は、通信部１１４を制御して、指示されたPCにアクセスする。

【０１３４】また、ローカルサーバ一覧画面２９１のローカルサーバ一覧表示欄２９２の右上に設けられた更新ボタン２９４を、ユーザがマウス等で操作すると、CPU１０１は、ローカルサーバ一覧表示欄２９２に表示されている情報を更新し、最新のPCの一覧情報を表示する。

【０１３５】さらにローカルサーバ一覧表示欄２９２の下側には、詳細情報表示ボタン２９５が設けられており、ユーザがマウス等でこの詳細情報表示ボタン２９５を操作すると、例えば、ローカルサーバ一覧表示欄２９２に表示されているPCのアドレス情報や機種情報等の詳細情報が表示される。また、ローカルサーバ一覧表示欄２９２に表示されているPCの登録を解除することもできる。ユーザが表示されたGUIに基づいてPCの登録を解除すると、ローカルサーバ一覧画面２９１のローカルサーバ一覧表示欄２９２からそのPCが削除される。

【０１３６】また、ローカルサーバ一覧画面２９１の右上部には、SSL解除ボタン２９６とログアウトボタン２９７が設けられている。

【０１３７】外部端末装置２２は、通常、ローカルサーバ１１にSSLを用いて情報を暗号化して接続を行う。ユーザがマウス等によりSSL解除ボタン２９６を操作すると、外部端末装置２２は、SSLによる暗号化を行わずにローカルサーバ１１と通信を行うことができる。これにより、SSLを用いた暗号化による負荷をかけずに通信を行うことができるので、例えば、外部端末装置２２の処理能力が高くない場合であっても、ローカルサーバ１１と通信を行うことができる。

【０１３８】また、ユーザがマウス等によりログアウトボタン２９７を操作すると、外部端末装置２２は、接続されている接続管理サーバ３１からログアウトし、ローカルサーバ１１への接続処理を中断する。

【０１３９】図１２に戻り、外部端末装置２２のユーザが、以上のようなローカルサーバ一覧画面２９１より接続するPCを選択し、接続を指示すると、外部端末装置２２のCPU１０１は、ステップＳ８３において、供給用データに基づいて、ローカルサーバ１１にアクセスする。CPU１０１は、指示されたPCのアクセス先の接続キーが付加されたURLを、取得した供給用データの中から参照し、そのURLにアクセスする。

【０１４０】ステップＳ９１において、外部端末装置２２よりネットワーク２１を介してアクセスされたローカルサーバ１１のCPU５１は、ステップＳ９２において、ログイン画面データを、ネットワーク２１を介して、外部端末装置２２に供給する。

【０１４１】外部端末装置２２のCPU１０１は、ステップＳ８４において、ローカルサーバ１１より供給されたログイン画面データを取得し、出力部１１２を制御して、ディスプレイ等に取得したログイン画面を表示させる。

【０１４２】図１５は、ディスプレイに表示されたログイン画面の例を示す図である。

【０１４３】図１５において、ディスプレイには、WEBブラウザ画面３０１が表示され、WEBブラウザ画面上にログイン画面３０２が表示される。ログイン画面３０２の中央には、外部端末装置２２のユーザが有するローカルサーバ用識別情報に含まれるユーザ名を入力するユーザ名入力欄３０３、同様に、ローカルサーバ用識別情報に含まれるパスワードを入力するパスワード入力欄３０４、ユーザがマウス等により操作することで、入力されたユーザ名およびパスワードをローカルサーバ１１に供給する処理の開始を指示するOKボタン３０５が設けられている。

【０１４４】ユーザは、キーボードまたはマウス等を操作して、ログイン画面３０２のユーザ名入力欄３０３に、ローカルサーバ１１に登録してあるユーザ名を入力し、パスワード入力欄３０４に、ローカルサーバ１１に登録してあるパスワードを入力し、OKボタン３０５を操作することで、ローカルサーバ１１にローカルサーバ用識別情報を供給することができる。

【０１４５】図１２に戻り、ユーザがログイン画面３０２に基づいて、ローカルサーバ用識別情報を入力して供給を指示すると、外部端末装置２２のCPU１０１は、ステップＳ８５において、通信部１１４を制御して、ネットワーク２１を介して、入力されたローカルサーバ用識別情報をローカルサーバ１１に供給する。

【０１４６】ローカルサーバ１１のCPU５１は、ステップＳ９３において、通信部６４を制御して、供給されたローカルサーバ用識別情報を取得し、ステップＳ９４において、取得したローカルサーバ用識別情報について、記憶部６３に記憶されているユーザに関する情報に基づいて、認証処理を行う。そして、認証処理が終了すると、CPU５１は、ステップＳ９５において、認証処理結果を外部端末装置２２に供給する。外部端末装置２２のCPU１０１は、供給された認証処理結果をステップＳ８６において取得する。

【０１４７】なお、例えば、接続キーが変更された（ログイン画面のURLが変更された）後で、外部端末装置２２が変更前の接続キーが付加されたURLにアクセスした場合、ローカルサーバ１１は、エラー処理結果を外部端末装置２２に供給し、接続を拒否する。外部端末装置２２は、取得したエラー処理結果に基づいて、図１６に示すように、「マイページから入りなおしてください」というエラーメッセージが表示されたエラー画面３１０を表示しているWEBブラウザ３０１をディスプレイに表示させる。

【０１４８】以上のように接続処理が行われることで、外部よりローカルサーバ１１のログイン画面にアクセスするためには、認証サービスプロバイダ３０の接続管理サーバ３１に接続し、ログイン画面のURLを取得しなければならない。すなわち、ローカルサーバ１１と通信を行うためには、認証サービスプロバイダ用識別情報およびローカルサーバ用識別情報が必要になり、より確実に不正なログインを抑制することができる。

【０１４９】また、ローカルサーバ１１のユーザは、図８の設定画面２５１において、接続キーの設定を行うことにより、セキュリティのレベルを自由に調節させることができる。例えば、接続キーが無効に設定された場合、外部端末装置２２は、ローカルサーバ１１のログイン画面のURLを取得していれば、ローカルサーバ用識別情報のみでローカルサーバ１１にログインすることができるし、固定の接続キーが有効に設定された場合、外部端末装置２２は、1度ローカルサーバ１１にログインするなどして、ローカルサーバ１１のログイン画面の接続キーが付加されたURLを取得していれば、ローカルサーバ用識別情報のみでローカルサーバ１１にログインすることができるし、決められた時間間隔で自動的に変更される接続キーに設定された場合、外部端末装置２２は、接続キーが変更されるたびに認証サービスプロバイダ３０の接続管理サーバ３１にログイン画面のURLを要求しなければならない。

【０１５０】また、外部端末装置２２のユーザが複数のローカルサーバにログインを許可されているような場合に置いても、ローカルサーバ１１のログイン画面のURLを認証サービスプロバイダ３０のアドレス管理サーバ３２が管理し、要求に対応するローカルサーバに関する情報をリストで供給するので、外部端末装置２２は、ログイン画面のURLを全て記憶しておく必要がなく、アドレス管理が容易である。

【０１５１】なお、以上においては、外部端末装置２２がローカルサーバ１１に接続する処理を説明したが、ネットワーク２１に接続されている基地局２４と無線通信を行い、ネットワーク２１に接続されている携帯電話機２３がローカルサーバ１１に接続する場合も、その処理は同様に行われる。

【０１５２】次に、このとき接続管理サーバによって実行されるアクセス制御処理を、図１７のフローチャートを参照して説明する。

【０１５３】最初に、ステップＳ１３１において、接続管理サーバ３１のCPU１５１は、通信部１６４を制御して、外部端末装置２２より認証サービスプロバイダ用識別情報を取得したか否かを判定することで、ローカルサーバ１１への接続を要求されたか否かを判定し、要求されたと判定するまで待機する。

【０１５４】認証サービスプロバイダ用識別情報を取得し、ローカルサーバ１１への接続を要求されたと判定した場合、CPU１５１は、ステップＳ１３２に進み、取得した認証サービスプロバイダ用識別情報について、認証処理を行う。CPU１５１は、認証処理として、取得した認証サービスプロバイダ用識別情報を認証サーバ３３に供給し、識別情報の認証を要求する。そして、認証サーバ３３より供給される認証結果を取得する。この処理

は、図１２のステップＳ１０２およびステップＳ１０３に対応する。

【０１５５】CPU１５１は、ステップＳ１３３において、取得した認証結果に基づいて、認証サービスプロバイダ用識別情報が認証されたか否かを判定する。認証されたと判定した場合、CPU１５１は、ステップＳ１３４において、認証された識別情報をアドレス管理サーバ３２に供給し、対応するローカルサーバ情報を要求する。この処理は、図１２のステップＳ１０４に対応する。

【０１５６】そして、ステップＳ１３５において、CPU１５１は、アドレス管理サーバ３２より要求したローカルサーバ情報を取得したか否かを判定し、取得したと判定するまで待機する。なお、所定の時間が経過した場合、または、エラーメッセージ等を取得した場合、CPU１５１は、アクセス制御処理を終了する。

【０１５７】要求したローカルサーバ情報を取得したと判定した場合、CPU１５１は、ステップＳ１３６に進み、取得したローカルサーバ情報に基づいて、供給用データを生成する。この処理は、図１２のステップＳ１０６に対応する。

【０１５８】供給用データを生成したCPU１５１は、ステップＳ１３７に進み、生成した供給用データを、ネットワーク２１を介して外部端末装置２２に供給し、アクセス制御処理を終了する。この処理は、図１２のステップＳ１０７に対応する。

【０１５９】また、ステップＳ１３３において、取得した認証結果に基づいて、認証サービスプロバイダ用識別情報が認証されていないと判定した場合、CPU１５１は、アクセス制御処理を終了する。

【０１６０】以上のようにして、ローカルサーバ１１に接続した外部端末装置２２は、ユーザの指示に基づいて、ネットワーク２１を介してローカルサーバ１１と通信を行い、ローカルサーバ１１に備えられているアプリケーションプログラムに要求することで、ローカルサーバ１１、またはLAN１２に接続されている端末装置１３等を制御することができる。

【０１６１】図１８は、外部端末装置２２およびローカルサーバ１１が有するアプリケーションプログラムの様子を示す図である。図１８を参照して、外部端末装置２２とローカルサーバ１１の通信の様子を説明する。

【０１６２】図１８において、ローカルサーバ１１には、WEBサーバ３２１が備えられており、このWEBサーバ３２１がHTTP等を利用した通信を行い、HTML文書や画像、音声等の各種の情報を、LAN１２およびネットワーク２１を介して外部端末装置２２とやり取りする。

【０１６３】また、WEBサーバ３２１には、SSLを用いた暗号化を行うSSL３２２が連携されており、WEBサーバ３２１は、このSSL３２２を用いて、外部端末装置２２に送信する送信データを暗号化したり、外部端末装置２２より供給された暗号化されている受信データを復号したりする。

【０１６４】また、ローカルサーバ１１には、各種のアプリケーションプログラムを動作させるためのフレームワーク３２３が設けられており、WEBサーバを介して供給される外部端末装置２２からの要求情報をアプリケーションプログラムに供給したり、アプリケーションプログラムの処理結果をWEBサーバ３２１を介して外部端末装置２２に供給したりする。

【０１６５】図１８においては、フレームワーク３２３には、図示せぬメールサーバに対してクライアント処理を行うメールクライアントプログラム３３１Ａ、アドレスに関する情報を管理し、例えば、メールクライアントプログラム３３１Ａと連携して動作するアドレス管理プログラム３３１Ｂ、ユーザの入力したスケジュールに関する情報を管理するスケジュール管理プログラム３３１Ｃ、および、その他のアプリケーションプログラムであるアプリケーションプログラム３３１Ｄ等が、搭載されている。フレームワーク３２３には、上述した以外にも、どのようなアプリケーションプログラムが搭載されていてもよく、また、搭載する数も、動作可能であれば、いくつでも良い。

【０１６６】フレームワーク３２３には、例えば、WEBコンテンツ３２４等が連携されており、フレームワーク３２３、またはフレームワーク３２３に搭載されたアプリケーションプログラムが必要とするヘルプ３３２Ａや画像３３２Ｂなどを提供する。なお、WEBコンテンツ３２４は、上述した以外のコンテンツを備えていてもよい。

【０１６７】フレームワーク３２３には、JAVA（登録商標）関連モジュール３２５が連携されており、JAVA（登録商標）関連モジュール３２５は、フレームワーク３２３、およびフレームワーク３２３に搭載されているアプリケーションプログラムが必要とするJAVA（登録商標）言語に関する機能を提供する。

【０１６８】LAN１２およびネットワーク２１を介してローカルサーバ１１と接続されている外部端末装置２２は、WEBブラウザ３４１を有しており、WEBブラウザ３４１を用いて、HTTP等を利用した通信を行い、HTML文書や画像、音声等の各種の情報をローカルサーバ１１とやり取りする。なお、図示は省略するが、WEBブラウザ３４１は、SSL機能を有しており、WEBサーバ３２１とSSLを用いた暗号通信をおこなうことができる。

【０１６９】以上のように、ローカルサーバ１１と外部端末装置２２は、WEBサーバ３２１とWEBブラウザ３４１により、HTTPを用いた通信を行う。

【０１７０】次に、ローカルサーバ１１と外部端末装置２２による通信処理を、図１９のタイミングチャートを参照して説明する。ここでは、外部端末装置２２がローカルサーバ１１のアプリケーションプログラム３３１Ｄを制御する場合を説明する。

【０１７１】最初に、外部端末装置２２のWEBブラウザ３４１は、ステップＳ１５１において、ユーザに指示された、画面表示や情報設定等の要求情報を、ネットワーク２１およびLAN１２を介して、ローカルサーバ１１のWEBサーバ３２１に供給する。

【０１７２】WEBサーバ３２１は、ステップＳ１６１において、WEBブラウザ３４１より供給された要求情報を取得すると、ステップＳ１６２において、取得した要求情報をフレームワーク３２３に供給する。

【０１７３】フレームワーク３２３は、ステップＳ１７１において、その要求情報を取得すると、まず、ステップＳ１７２において、要求情報を供給した外部端末装置２２のユーザの認証処理を実行する。認証処理は、例えば、要求情報を供給する際に用いられる接続キーや、要求情報に含まれるユーザの識別情報等により行われる。そして、ユーザが認証されると、フレームワーク３２３は、ステップＳ１７３において、取得した要求情報をXML（eXtensible Markup Language）ドキュメント化し、ステップＳ１７４において、XMLドキュメント化した要求情報を、対応するアプリケーションプログラム３３１Ｄに供給する。

【０１７４】図２０は、フレームワーク３２３によりXMLドキュメント化された要求情報の例を示す図である。

【０１７５】図２０において、上から1行目には、XMLのバージョンやエンコード方式等の基本情報が構成されている。3行目乃至6行目には、接続してきた装置の機種に関する情報、アドレスに関する情報等を含む接続情報が構成されている。

【０１７６】そして、上から7行目および９行目には、ユーザのIDおよびパスワード、並びに、そのユーザ用のファイルが存在するフォルダに関する情報等を含む、接続してきたユーザに関する情報が構成されている。また、8行目には、処理要求として入力された情報が構成されている。さらに、１０行目乃至１３行目には、アプリケーションがフレームワークに要求する事項を入力する場所が、XML文書の位置特定に用いる記法であるXPathにより記載されている。

【０１７７】以上のような、アプリケーションプログラムに供給される要求情報は、XMLドキュメント化されており、必要な情報は全て構成されるようにし、項目や行数などのデータ構造に関する制限は特にない。アプリケーションは、XMLドキュメントを取り扱うことができればよく、全てのアプリケーションプログラムが読み込み可能な共通化されたデータ構造を用意する必要はない。すなわち、例えば、フレームワーク３２３に新たにアプリケーションプログラムを追加する際も、その追加するアプリケーションプログラムが読み込むデータ構造が、先に搭載されているアプリケーションプログラムが読み込むデータ構造と共通である必要がなく、汎用性が高い。

【０１７８】従って、例えば、規格の変更などにより、最新のアプリケーションプログラムに必要なデータが、これまでのアプリケーションプログラムが利用していたデータ構造と異なる場合においても、フレームワークを変更することなく最新のアプリケーションプログラムを追加することができる。

【０１７９】図１９に戻り、以上のようにXMLドキュメント化された要求情報を、アプリケーションプログラム３３１Ｄは、ステップＳ１８１において取得し、ステップＳ１８２において、取得した要求情報に基づいて、要求された固有の処理を行い、ステップＳ１８３において、要求情報に対応する応答情報を生成する。

【０１８０】アプリケーションプログラム３３１Ｄは、例えば、現在接続しているユーザ用のファイルのあるフォルダや要求内容などの使用する各種情報をフレームワーク３２３より供給されるXMLドキュメント化された要求情報から取得する。要求情報に関して、必要な情報解析はフレームワーク３２３が行っているので、アプリケーションプログラム３３１Ｄは、XMLドキュメント化された要求情報のXPathで記述された内容に従って、必要な情報を取得することができる。

【０１８１】そして、アプリケーションプログラム３３１Ｄは、ステップ１８４において、生成した応答情報に、画面表示に関する表示情報を付加した後、ステップＳ１８５において、その表示情報を付加した応答情報をフレームワーク３２３に供給する。

【０１８２】図２１は、アプリケーションプログラム３３１Ｄよりフレームワーク３２３に供給される応答情報の例を示す図である。

【０１８３】図２１において、上から１行目乃至９行目は、図２０に示す内容と動揺であるので、その説明は省略する。１０行目乃至１４行目はフレームワーク３２３への要求が設定されており、１６行目以降はアプリケーション固有の情報設定により構成されている。

【０１８４】アプリケーションプログラム３３１Ｄより出力される応答情報は、フレームワークを介して、要求情報の要求元である端末装置に供給される。従って、要求もとの端末装置の表示部の大きさ等により、表示される内容や形式が異なってしまう。しかしながら、アプリケーションプログラム３３１Ｄは、要求情報を供給した端末装置の機種が何かを特に必要でない限り意識せずに、必要とされる情報を全てXMLドキュメントに追加するようにし、要求元である端末装置に最適な情報は、フレームワーク３２３が、アプリケーションプログラムより供給された応答情報を編集することにより、作成するようにする。

【０１８５】図１９に戻り、以上のような、アプリケーションプログラム３３１Ｄに供給された応答情報は、ステップＳ１７５において、フレームワーク３２３に取得される。そして、フレームワーク３２３は、ステップＳ

１７６において、取得した応答情報に基づいて、要求情報の供給元に最適な出力用応答情報を生成し、ステップＳ１７７において、生成した出力用応答情報を供給する。すなわち、フレームワーク３２３は、応答情報を解析し、要求情報の供給元のWEBブラウザの種類等に応じて、最適な出力画像構成となるように、使用するXSL（eXtensible Stylesheet Language）を変更し、HTMLドキュメントを生成する。なお、フレームワーク３２３は、HTMLドキュメントを生成するとともに、応答情報を解析し、要求情報の供給元のWEBブラウザの種類等に応じて、出力画像が最適なレイアウトとなるように、使用するCSS（Cascading Style Sheet）を変更するようにしてもよい。

【０１８６】WEBサーバ１６３は、ステップＳ１６３において、フレームワーク３２３に供給された出力用応答情報を取得すると、ステップＳ１６４において、取得した出力用応答情報を要求情報の供給元である外部端末装置２２に供給する。外部端末装置２２は、ステップＳ１５２において、供給された出力用応答情報を取得し、ディスプレイ等に表示させる。

【０１８７】以上のようにして、ローカルサーバ１１と外部端末装置２２は、通信処理を行う。以上においては、外部端末装置２２がローカルサーバ１１のアプリケーションプログラム３３１Ｄを制御するように説明したが、これに限らず、外部端末装置２２が制御するアプリケーションプログラムは、フレームワーク３２３に搭載されるアプリケーションプログラムであれば何でも良い。また、携帯電話機２３がローカルサーバ１１と通信処理を行う場合も、上述した場合と同様の処理が行われる。

【０１８８】次に、この通信処理において行われる、フレームワーク３２３によるアプリケーションプログラム管理処理を、図２２のフローチャートを参照して説明する。

【０１８９】フレームワーク３２３は、ステップＳ２０１において、WEBサーバ３２１より要求情報を取得したか否かを判定し、取得したと判定するまで待機する。そして、取得したと判定した場合、フレームワーク３２３は、ステップＳ２０２に進み、取得した要求情報に対して、上述したような認証処理が必要か否かを判定する。

【０１９０】認証処理が必要と判定した場合、フレームワーク３２３は、ステップＳ２０３に進み、取得した要求情報に対して認証処理を行う。この処理は、図１９のステップＳ１７２の処理に対応する。そして、フレームワーク３２３は、ステップＳ２０４に進み、要求情報の供給元のユーザが認証されたか否かを判定する。

【０１９１】認証されたと判定した場合、フレームワーク３２３は、ステップＳ２０５に進む。また、ステップＳ２０２において、認証処理が必要でないと判定した場合、フレームワーク３２３は、ステップＳ２０５に進む。

【０１９２】ステップＳ２０５において、フレームワーク３２３は、取得した要求情報を、上述したように、XMLドキュメント化する。この処理は、図１９のステップＳ１７３の処理に対応する。

【０１９３】要求情報をXMLドキュメント化したフレームワーク３２３は、ステップＳ２０６において、フレームワーク３２３に対応する要求情報が存在するか否かを判定し、存在すると判定した場合は、ステップＳ２０７に進み、要求情報に基づいて、必要な処理を行い、ステップＳ２０８に進む。ステップＳ２０６において、フレームワーク３２３に対応する要求情報が存在しないと判定した場合、フレームワーク３２３は、そのまま、ステップＳ２０８に進む。

【０１９４】ステップＳ２０８において、フレームワーク３２３は、アプリケーションプログラムに供給する要求情報が存在するか否かを判定し、存在すると判定した場合、ステップＳ２０９に進み、要求情報を対応するアプリケーションプログラムに供給する。この処理は、図１９のステップＳ１７４の処理に対応する。

【０１９５】要求情報を供給したフレームワーク３２３は、ステップＳ２１０に進む。また、ステップＳ２０８において、アプリケーションプログラムに供給する要求情報が存在しないと判定した場合、フレームワーク３２３は、ステップＳ２１０に進む。ステップＳ２１０において、フレームワーク３２３は、要求情報を供給したアプリケーションプログラムより応答情報を取得したか否かを判定し、取得した、若しくは要求情報を供給していないと判定するまで待機する。

【０１９６】応答情報を取得した、または、要求情報を供給していないと判定した場合、フレームワーク３２３は、ステップＳ２１１に進む。また、ステップＳ２０４において、ユーザが認証されなかったと判定した場合、フレームワーク３２３は、ステップＳ２１１に進む。

【０１９７】ステップＳ２１１において、フレームワーク３２３は、取得した応答情報に基づいて、最適な出力用応答情報を生成する。この処理は、図１９のステップＳ１７６の処理に対応する。最適な出力用応答情報を生成したフレームワーク３２３は、ステップＳ２１２に進み、生成した出力用応答情報をWEBサーバ３２１に供給し、アプリケーションプログラム管理処理を終了する。

【０１９８】以上のように通信処理を行い、外部端末装置２２がローカルサーバ１１のメールクライアントプログラム３３１Ａを制御し、ローカルエリア１０の外部からローカルサーバ１１が受信した電子メールを参照する場合の処理を図２３のタイミングチャートを参照して説明する。必要に応じて、図２４乃至図２６を適宜参照して説明する。

【０１９９】まず、図１８に示すメールクライアントプログラム３３１Ａは、ステップＳ２５１において、メー

ルサーバにアクセスし、まだ、受信していない電子メールである未受信メールを要求する。この処理は、予め登録された設定に基づいて、所定の時間間隔で、自動的に、繰り返し行われる。

【０２００】メールサーバは、ステップＳ２４１において、メールクライアントプログラム３３１Ａからの要求を取得すると、未受信メールがある場合、ステップＳ２４２において、要求された未受信メールをメールクライアントプログラム３３１Ａに供給する。メールクライアントプログラム３３１Ａは、ステップＳ２５２において、供給された電子メールを取得すると、ステップＳ２５３において、取得したメールを保存する。

【０２０１】ローカルエリア１０の外部に存在する外部端末装置２２は、ユーザの指示により、ステップＳ２３１において、ネットワーク２１を介してローカルサーバ１１にアクセスし、ユーザのアカウントに対応するメールを要求する。

【０２０２】図２４は、外部端末装置２２のディスプレイに表示されるメールクライアントトップ画面の例を示す図である。外部端末装置２２がネットワーク２１を介してローカルサーバ１１にアクセスすると、上述したように認証処理が行われ、ローカルサーバ１１のフレームワーク３２３は、メールクライアントプログラム３３１を動作させ、応答情報として、図２４に示すようなGUI情報を外部端末装置２２に供給する。外部端末装置２２のCPU１０１は、出力部１１２を制御して、取得したGUI情報を、ディスプレイに表示されているWEBブラウザ画面３０１に表示させる。

【０２０３】図２４において、WEBブラウザ画面３０１には、メールクライアントトップ画面３５１が表示されている。メールクライアントトップ画面３５１は、メールクライアントプログラム３３１Ａが供給するGUIの中で最も上位のGUIであり、メールクライアントプログラム３３１Ａが提供する各種の機能を実行させるボタンやリンクにより構成されている。すなわち、外部端末装置２２のユーザは、メールクライアントトップ画面３５１を構成するリンクやボタンを操作することで、例えば、受信した電子メールの一覧を表示する受信箱を表示させたり、新規に電子メールを作成する画面を表示させたりすることができる。

【０２０４】メールクライアントトップ画面３５１の上部には、例えば、ユーザがマウス等により操作することで、新規の電子メールを作成する際に使用するアドレス帳の機能を動作させるアドレス帳ボタン３５２や、着信した電子メールの通知や転送先のアドレスを設定する機能を動作させる通知・転送設定ボタン３５３等を含む各種の機能を実行するボタン群が形成されている。

【０２０５】メールクライアントトップ画面３５１の左側には、メールクライアントプログラム３３１Ａが提供する機能の一覧がリンクとして表示されている機能選択欄３５４が構成されており、ユーザはマウス等によりこれらのリンクを指示することによっても各種の機能を実行させることができる。

【０２０６】また、メールクライアントトップ画面３５１の中央には、主な機能を動作させるボタン群およびその説明で構成されるメインメニュー欄３５５が形成されている。ユーザは、マウス等によりメインメニュー欄３５５に含まれるボタンを操作することによっても動作させる機能を選択することができる。

【０２０７】外部端末装置２２のユーザは、以上のようなGUI画面に基づいて、メールクライアントプログラム３３１Ａに対する要求を指示する。例えば、ユーザが受信箱の表示を要求すると、外部端末装置２２は、その要求を、ステップＳ２３１において、メールクライアントプログラム３３１Ａに供給する。この要求は、ローカルサーバ１１に供給され、上述したように処理が行われ、メールクライアントプログラム３３１Ａに供給される。

【０２０８】ステップＳ２５４において、その要求を取得したメールクライアントプログラム３３１Ａは、上述したように、固有の処理を行い、保存済みメール一覧に関する情報を供給する。外部端末装置２２は、ステップＳ２３２において、供給された保存済みメール一覧に関する情報を取得すると、図２５に示すように、取得した保存済みメール一覧をディスプレイ等に表示させる。

【０２０９】図２５は、外部端末装置２２のディスプレイに表示された受信箱画面の例を示す図である。

【０２１０】外部端末装置２２のディスプレイに表示されているWEBブラウザ画面３０１には、ローカルサーバ１１のメールクライアントプログラム３３１Ａより供給された保存済みメールの一覧を表示する受信箱画面３６１が構成されている。

【０２１１】受信箱画面３６１には、保存済みメールの一覧からなる受信メール選択欄３６２が構成されている。受信メール選択欄３６２は、未読または既読等の状態を示す項目、添付ファイルの有無を示す項目、電子メールの差出人の名前を示す項目、電子メールの件名を示す項目、および、着信日付または送信日付を示す項目等により構成されている。

【０２１２】受信メール選択欄３６２に表示されている内容のうち一部または全部がリンクにより構成されており、外部端末装置２２のユーザは、例えば、受信メール選択欄３６２に表示されている電子メールの中から目的の電子メールの件名を、マウス等を操作することにより選択することにより、その電子メールの本文等を表示させることができる。

【０２１３】図２３に戻り、ユーザが図２５に示す受信メール選択欄３６２の中から目的のメールを選択すると、外部端末装置２２は、ステップＳ２３３において、取得した保存メール一覧の中から、ユーザに指示された電子メールを選択し、その電子メールを供給するよう

に、メールクライアントプログラム３３１Ａに要求する。

【０２１４】外部端末装置２２のWEBブラウザ３４１からの要求は、WEBサーバ３２１およびフレームワーク３２３を介して、メールクライアントプログラム３３１Ａに供給される。メールクライアントプログラム３３１Ａは、ステップＳ２５６において、その要求を取得する。外部端末装置２２からの要求を取得したメールクライアントプログラム３３１Ａは、要求に対応する処理を行い、ステップＳ２５７において、要求された電子メールを外部端末装置２２に供給する。

【０２１５】外部端末装置２２は、ステップＳ２３４において、供給された電子メールを取得すると、ディスプレイ等に表示させる。

【０２１６】図２６は、外部端末装置２２のディスプレイに表示されたメール表示欄の例を示す図である。

【０２１７】図２６において、WEBブラウザ画面３０１には、電子メールの本文等を表示するメール表示欄３７１が表示されている。メール表示欄３７１には、電子メールの本文の他に、電子メールの日付、差出人、宛先、同報、件名、および添付ファイルに関する情報等が表示される。

【０２１８】外部端末装置２２のユーザは、このメール表示欄３７１を参照することにより、ローカルサーバ１１において受信した電子メールの内容を見ることができる。これにより、例えば、ユーザは、自宅に設置されているローカルサーバ１１のメールクライアント３３１Ａが受信した電子メールを、外出先においても読むことが可能となる。

【０２１９】以上においては、メールクライアントプログラム３３１Ａが受信した電子メールをローカルエリア１０の外部において取得する処理を説明したが、これに限らず、外部端末装置２２のユーザは、上述した処理と同様の処理を行うことにより、例えば、メールクライアントプログラム３３１Ａに登録してあるアカウントで送信メールを作成したり、受信メールをフォルダに分類する等して整理したり、メールクライアントプログラム３３１Ａに関する各種の設定を変更したりする等の、メールクライアントプログラム３３１Ａが有する様々な機能を制御することができる。

【０２２０】また、以上においては、メールクライアントプログラム３３１Ａが予め受信した電子メールを、外部端末装置２２がユーザの指示に基づいてローカルサーバ１１にアクセスし、取得するように説明したが、これに限らず、電子メールを受信した場合、自動的に、メールクライアントプログラム３３１Ａが受信した旨を通知したり、受信したメールを外部端末装置２２に転送したりするようにしてもよい。

【０２２１】その場合、ユーザは、メールクライアントプログラム３３１Ａが電子メール受信時に、外部端末装置２２に対して、その旨を通知する、または受信した電子メールを転送するように予め設定しておく。外部端末装置２２のユーザがマウス等により、外部端末装置２２は、ディスプレイ等に、図２４に示す通知・転送設定ボタン３５３を操作すると、図２７に示すような、通知・転送に関する設定を行う通知・転送リスト表示欄を表示させる。

【０２２２】図２７は、WEBブラウザ画面に表示されている通知・転送リスト表示欄を示す図である。

【０２２３】図２７において、ディスプレイに表示されているWEBブラウザ画面３０１には、電子メール受信時の通知、または転送に関する設定の一覧が表示されている通知転送リスト表示欄３８１が表示されている。

【０２２４】通知・転送リスト表示欄３８１には、これまでに設定された通知および転送に関する設定情報の一覧の他に、ユーザがマウス等により操作することで、新規に設定情報を追加するGUIをWEBブラウザ画面３０１に表示させる追加ボタン３８２、ユーザがマウス等により操作することで、既に設定され、一覧に表示されている設定情報を削除するボタン等が設けられている。

【０２２５】外部端末装置２２のユーザは、マウス等を用いて追加ボタン３８２を操作することにより、図２８に示すような、通知または転送の設定を行うことができる通知・転送先設定欄をWEBブラウザ画面３０１に表示させ、新たな設定情報を作成することができる。

【０２２６】図２８は、WEBブラウザ画面に表示されている通知・転送先設定欄を示す図である。

【０２２７】図２８において、ディスプレイに表示されているWEBブラウザ画面３０１には、電子メール受信時の通知、または転送に関する設定を行うことができる通知転送先設定欄３９１が表示されている。

【０２２８】通知・転送先設定欄３９１には、ユーザがマウスまたはキーボード等を用いて通知・転送に関する設定情報の名前を入力するデータ名入力欄３９２、ユーザがマウス等を用いて、この設定情報が指示する処理の内容を選択するアクション選択欄３９３、ユーザがマウスまたはキーボード等を用いて、通知または転送先のアドレスを入力する通知・転送先アドレス入力欄３９４、および、ユーザがマウスまたはキーボード等を用いて、この設定情報に関するコメント等を入力するコメント入力欄３９５等が設けられている。また、これ以外にも、ユーザがマウス等を用いて操作することにより、入力した設定情報を新たに登録する追加ボタン等が構成されていても良い。

【０２２９】外部端末装置２２のユーザは、この通知・転送先設定欄３９１に基づいて、通知または転送に関する設定情報を入力し、予め登録しておくことができる。

【０２３０】WEBブラウザ画面３０１に表示された、以上に示すようなGUI画面に基づいて、受信時に通知を行うようにする設定が予め行われている場合の処理を、図

２９のタイミングチャートを参照して説明する。

【０２３１】図２３に示す場合と同様に、ステップＳ２９１において、メールクライアントプログラム３３１Ａが予め定められた時間間隔で、未受信メールを要求すると、メールサーバは、ステップＳ２８１において、その要求を取得し、ステップＳ２８２において、要求に対応する未受信メールが存在する場合、その未受信メールをメールクライアントプログラム３３１Ａに供給する。

【０２３２】メールクライアントプログラム３３１Ａは、ステップＳ２９２において、供給された電子メールを取得すると、ステップＳ２９３において、所得した新規受信メールを通知する通知メールを生成する。

【０２３３】そして、ステップＳ２９４において、メールクライアントプログラム３３１Ａは、生成した通知メールを、ネットワーク２１を介して、外部端末装置２２に供給する。外部端末装置２２は、ステップＳ２７１において、その通知メールを取得し、ディスプレイに表示されているWEBブラウザ３０１に、図２６に示すようなメール表示欄３７１に取得した通知メールを表示する。

【０２３４】外部端末装置２２が取得した通知メールには、メールクライアントプログラム３３１Ａが電子メールを受信した旨を知らせるメッセージの他に、受信メールの件数、件名、または差出人などの、受信メールに関する主な情報、並びに、外部端末装置２２が通知メールに対応する受信メールを取得する際にアクセスするアクセス先のURLが含まれていてもよい。

【０２３５】また、このURLはリンクになっていてもよく、ユーザがブラウザ画面３０１に表示されているこのURLを、マウス等を用いて選択することにより、外部端末装置２２が、選択されたURLにアクセスし、対応する受信メールを表示するようにしてもよい。この場合、外部端末装置２２が、ユーザにより選択されたURLにアクセスすると、ディスプレイに表示されているWEBブラウザ画面３０１には、対応する受信メールが表示された、図２６に示すようなメール表示欄３７１が表示される。

【０２３６】このとき、通知メールに含まれるURLには、上述したような接続キーが含まれており、図１に示す認証サービスプロバイダ３０による認証処理を省略することができる。また、同様に、通知メールに含まれるURLにローカルサーバ用識別情報が含まれるようにし、ローカルサーバ１１による認証処理も省略するようにしてもよい。

【０２３７】以上のようにすることにより、外部端末装置２２のユーザは、取得した通知メールに含まれるURLのリンクを、マウス等を用いて選択するだけで、ローカルサーバ１１のメールクライアントプログラム３３１Ａが受信したメールをディスプレイに表示させ、閲覧することができる。

【０２３８】なお、それとは逆に、URLに接続キーが含まれないようにして、外部端末装置２２のユーザが受信メールを閲覧する際に、認証サービスプロバイダ３０の認証処理が必要であるようにしてもよい。

【０２３９】通知メールを取得し、ディスプレイ等に表示させた外部端末装置２２は、ステップＳ２７２において、取得した通知メールに基づいてローカルサーバ１１にアクセスし、ユーザの指示に対応するメールを、メールクライアントプログラム３３１Ａに要求する。

【０２４０】メールクライアントプログラム３３１Ａは、ステップＳ２９５において、その要求を取得すると、ステップＳ２９６において、要求されたメールを外部端末装置２２に供給する。外部端末装置２２は、ステップＳ２７３において、供給された電子メールを取得し、ディスプレイ等にその内容を表示する。

【０２４１】以上のように処理が行われることにより、外部端末装置２２のユーザは、ローカルエリア１０の外部より、メールクライアントプログラム３３１Ａが受信したメールを閲覧することができる。

【０２４２】以上においては、外部端末装置２２がネットワーク２１を介してローカルサーバ１１に接続し、メールクライアントプログラム３３１Ａを制御するように説明したが、これに限らず、外部端末装置２２が制御するアプリケーションプログラムは、メールクライアントプログラム３３１Ａ以外にも、例えば、アドレス管理プログラム３３１Ｂやスケジュール管理プログラム３３１Ｃなどのように、ローカルサーバ１１が有するアプリケーションプログラムであればなんでもよい。

【０２４３】図３０は、WEBブラウザ画面３０１に表示されたアドレス帳トップ画面の例を示す図である。

【０２４４】図３０において、ディスプレイに表示されたWEBブラウザ画面３０１には、アドレス管理サーバ３３１Ｂに対応するGUIのトップ画面であるアドレス帳トップ画面４０１が表示されている。

【０２４５】アドレス帳トップ画面４０１には、ユーザがマウス等を用いて操作することにより、アドレス管理プログラム３３１Ｂの主な機能の制御を行うGUIを表示させることができるメインメニュー画面４０２、および、ユーザがマウス等を用いて選択することにより、アドレス管理プログラム３３１Ｂが提供するアドレス帳機能に属する各種の機能の制御を行うGUIを表示させることができるリンク群である機能選択欄４０３が含まれている。

【０２４６】ユーザは、このアドレス帳トップ画面４０１の各種のボタンまたはリンクを操作することにより、アドレス帳を開いたり、アドレス情報を編集したりすることができる。

【０２４７】以上のようにして、外部端末装置２２のユーザは、ローカルエリア１０の外部より、ネットワーク２１を介して、ローカルサーバ１１に接続し、各種のアプリケーションプログラムを制御することができ、それにより、ローカルサーバ１１、および、LAN１２に接続

されている端末装置１３等の動作を制御することができる。

【０２４８】なお、外部端末装置２２が制御可能なローカルサーバ１１のアプリケーションプログラムは、上述したもの以外にも、例えば、テレビジョン信号の録画や再生を行うアプリケーションプログラム、画像データの配信や編集などを行うアプリケーションプログラム、音楽データの録音や再生を行うアプリケーションプログラム等、図１８に示すフレームワーク３２３に搭載されているアプリケーションプログラムであれば、どのような機能を有するアプリケーションプログラムであってもよい。

【０２４９】以上においては、外部端末装置２２がローカルサーバ１１に接続し、各種のアプリケーションプログラムを制御するように説明したが、携帯電話機２３がローカルサーバ１１に接続し、各種のアプリケーションプログラムを制御する場合も、上述した場合と同様の処理が行われる。

【０２５０】また、ローカルエリア１０の外部の端末装置としては、上述したパーソナルコンピュータ等の外部端末装置２２、および携帯電話機２３の他に、例えば、通信機能を有するPDA（Personal Digital Assistance）などであってもよい。

【０２５１】以上において、図１に示すネットワークシステムを構成する、ローカルサーバ１１、端末装置１３、外部端末装置２２、携帯電話機２３、接続管理サーバ３１、アドレス管理サーバ３２、および認証サーバ３３は、それぞれ1台ずつで構成されるように説明したが、これに限らず、複数台により構成されていてもよい。また、認証サービスプロバイダ３０に設置された各サーバおよび各装置は、それぞれ、別体として構成してあるが、サービス全体、またはその一部が、一体化されていてもよい。

【０２５２】なお、以上において、システムとは、複数の装置により構成される装置全体を表すものである。

【０２５３】上述した一連の処理は、ハードウエアにより実行させることもできるが、ソフトウエアにより実行させることもできる。一連の処理をソフトウエアにより実行させる場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０２５４】この記録媒体は、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フロッピディスクを含む）、光ディスク（CD-ROM(Compact Disk-Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク（ＭＤ（Mini-Disk）を含む）、もしくは半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROMなどで構成される。

【０２５５】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２５６】

【発明の効果】以上のように、本発明のネットワークシステムによれば、より安全に通信を行うことができる。

【０２５７】本発明の第１の情報処理装置および方法、記録媒体、並びにプログラムによれば、より安全に他の情報処理装置と通信を行うことができる。

【０２５８】本発明の第２の情報処理装置および方法、記録媒体、並びにプログラムによれば、他の情報処理装置間の通信を容易に管理することができる。

【図面の簡単な説明】

【図１】本発明を適用したネットワークシステムの構成例を示す図である。

【図２】図１に示すローカルサーバの構成例を示すブロック図である。

【図３】図１に示す外部端末装置の構成例を示すブロック図である。

【図４】図１に示す接続管理サーバの構成例を示すブロック図である。

【図５】図１に示すアドレス管理サーバの構成例を示す図である。

【図６】図１に示すローカルサーバによるローカルサーバ情報登録処理を説明するフローチャートである。

【図７】図１に示すアドレス管理サーバによるローカルサーバ情報登録処理を説明するフローチャートである。

【図８】接続キーに関する設定を行う設定画面の様子の例を示す図である。

【図９】接続キーに関する設定を行う設定画面の様子の他の例を示す図である。

【図１０】図１に示すローカルサーバによるローカルサーバ情報更新処理を説明するフローチャートである。

【図１１】図１に示すアドレス管理サーバによるローカルサーバ情報更新処理を説明するフローチャートである。

【図１２】外部端末装置からローカルサーバにログインする処理を説明するタイミングチャートである。

【図１３】ログイン画面の例を示す図である。

【図１４】ローカルサーバ一覧画面の例を示す図である。

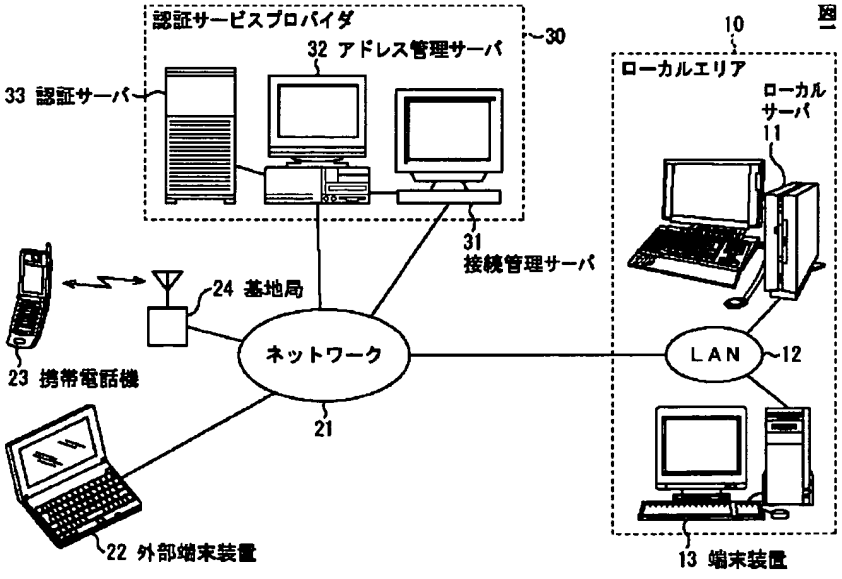
【図１５】ログイン画面の例を示す図である。

【図１６】エラー画面の例を示す図である。

【図１７】接続管理サーバによるアクセス制御処理を説

明するフローチャートである。
【図１８】アプリケーションプログラムの様子を示す図である。
【図１９】ローカルサーバと外部端末装置による通信処理を説明するタイミングチャートである。
【図２０】フレームワークによりXMLドキュメント化された要求情報の例を示す図である。
【図２１】フレームワークに供給される応答情報の例を示す図である。
【図２２】フレームワークによるアプリケーションプログラム管理処理を説明するフローチャートである。
【図２３】ローカルエリアの外部からローカルサーバが受信した電子メールを参照する場合の処理を説明するタイミングチャートである。
【図２４】メールクライアントトップ画面の例を示す図である。
【図２５】受信箱画面の例を示す図である。
【図２６】メール表示欄の例を示す図である。
【図２７】通知・転送リスト表示欄を示す図である。
【図２８】通知・転送先設定欄を示す図である。
【図２９】受信時に通知を行うようにする設定が予め行われている場合の処理を説明するタイミングチャートである。
【図３０】アドレス帳トップ画面の例を示す図である。
【符号の説明】
１１　ローカルサーバ，　１２　LAN，　１３　端末装置，　２１　ネットワーク，　２２　外部端末装置，　２３　携帯電話機，　２４　基地局，　３０認証サービスプロバイダ，　３１　接続管理サーバ，　３２　アドレス管理サーバ，　３３　認証サーバ，　３２１　WEBサーバ，　３２２　SSL，　３２３　フレームワーク，　３２４　WEBコンテンツ，　３２５　JAVA（登録商標）関連モジュール，　３３１Ａ　メールクライアントプログラム，　３３１Ｂ　アドレス管理プログラム，　３３１Ｃ　スケジュール管理プログラム，　３３１Ｄ　アプリケーションプログラム

【図１】



【図２】

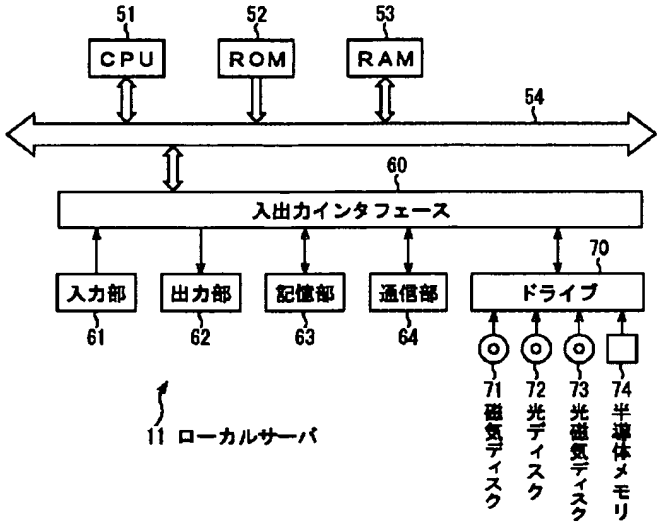

51
52
53
CPU
ROM
RAM
54
60
入出力インタフェース
70
入力部
出力部
記憶部
通信部
ドライブ
61
62
63
64
71 磁気ディスク
72 光ディスク
73 光磁気ディスク
74 半導体メモリ
11 ローカルサーバ

図2

【図３】

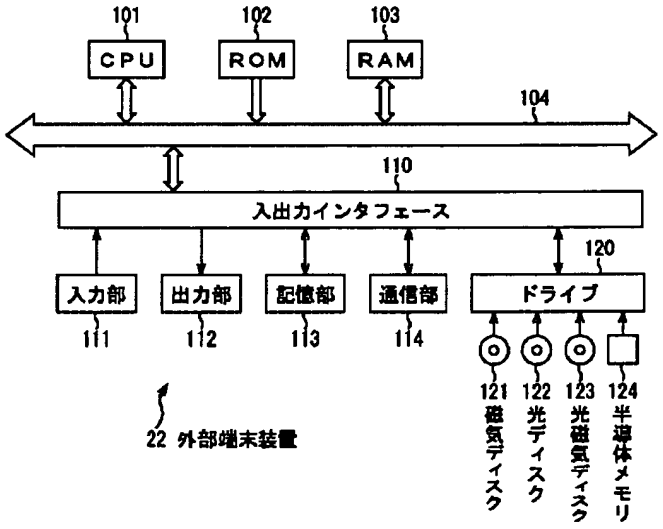

101
102
103
CPU
ROM
RAM
104
110
入出力インタフェース
120
入力部
出力部
記憶部
通信部
ドライブ
111
112
113
114
121 磁気ディスク
122 光ディスク
123 光磁気ディスク
124 半導体メモリ
22 外部端末装置

図3

【図４】

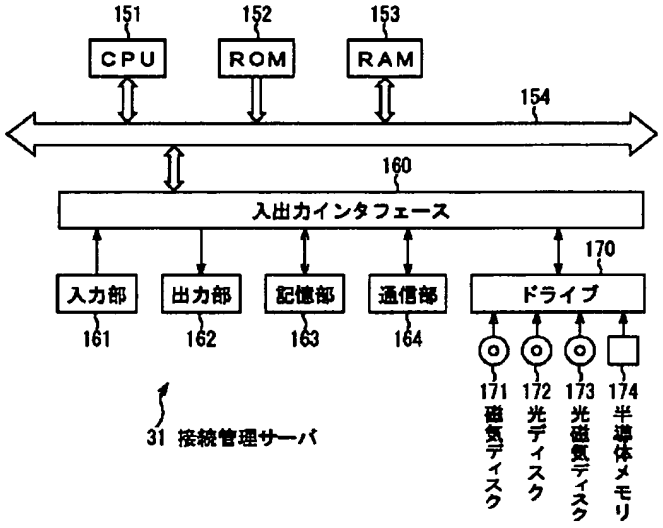

151
152
153
CPU
ROM
RAM
154
160
入出力インタフェース
170
入力部
出力部
記憶部
通信部
ドライブ
161
162
163
164
171 磁気ディスク
172 光ディスク
173 光磁気ディスク
174 半導体メモリ
31 接続管理サーバ

図4

【図５】

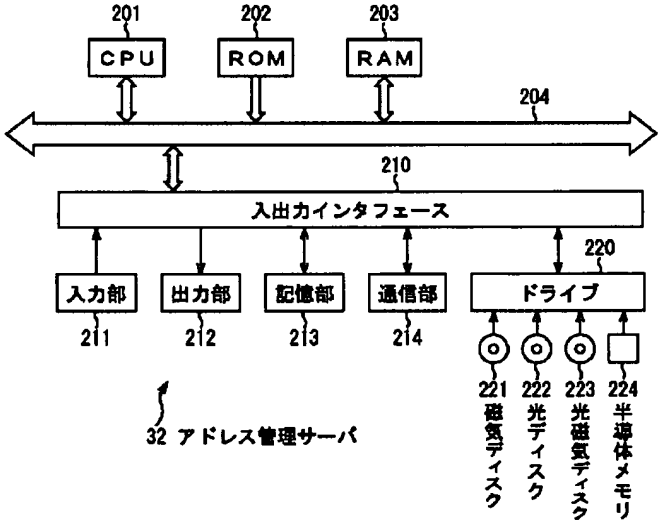
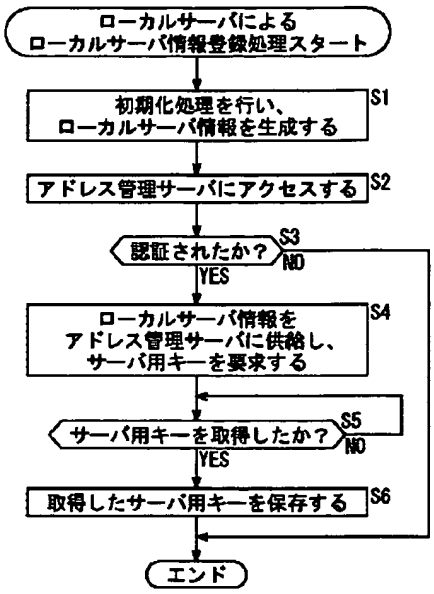

201
202
203
CPU
ROM
RAM
204
210
入出力インタフェース
220
入力部
出力部
記憶部
通信部
ドライブ
211
212
213
214
221 磁気ディスク
222 光ディスク
223 光磁気ディスク
224 半導体メモリ
32 アドレス管理サーバ

図5

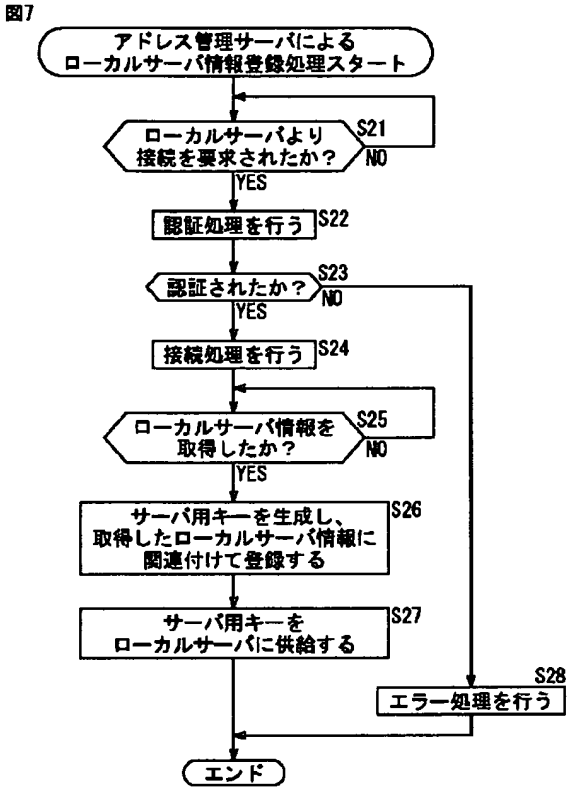
【図６】

図6



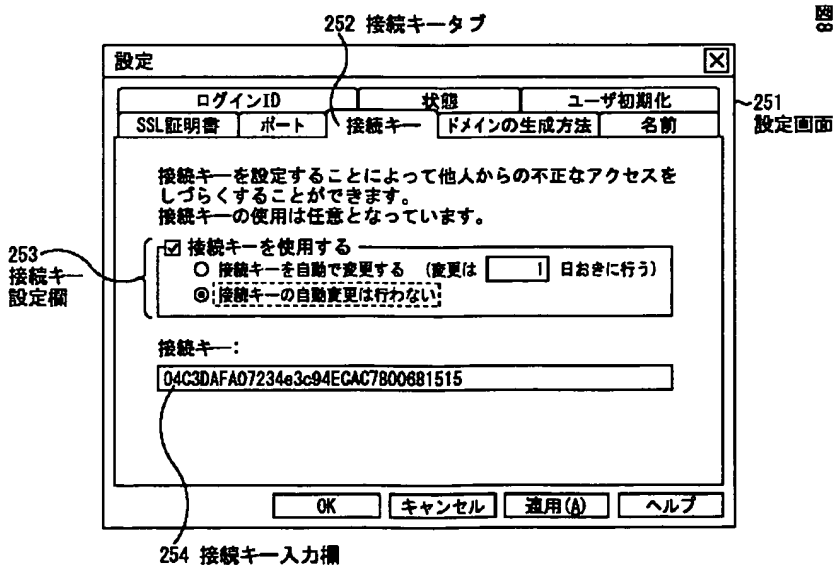
【図７】

図7



【図８】

図8



【図９】

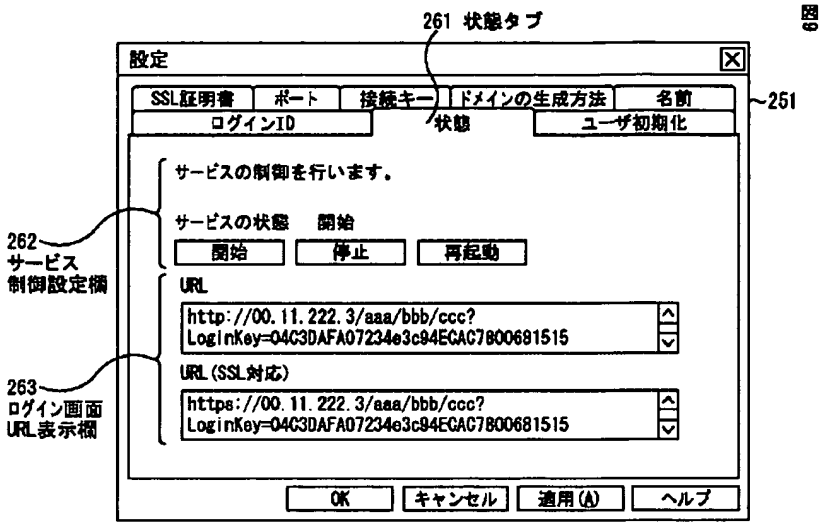


図9
261 状態タブ
設定
SSL証明書
ポート
接続キー
ドメインの生成方法
名前
ログインID
状態
ユーザ初期化
251
サービスの制御を行います。
サービスの状態　開始
開始
停止
再起動
262
サービス
制御設定欄
URL
http://00.11.222.3/aaa/bbb/ccc?
LoginKey=04C3DAFA07234e3c94ECAC7800681515
URL(SSL対応)
https://00.11.222.3/aaa/bbb/ccc?
LoginKey=04C3DAFA07234e3c94ECAC7800681515
263
ログイン画面
URL表示欄
OK
キャンセル
適用(A)
ヘルプ

【図１０】

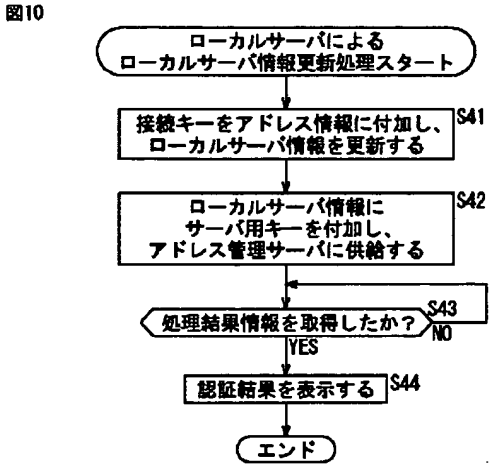


図10
ローカルサーバによる
ローカルサーバ情報更新処理スタート
接続キーをアドレス情報に付加し、
ローカルサーバ情報を更新する
S41
ローカルサーバ情報に
サーバ用キーを付加し、
アドレス管理サーバに供給する
S42
処理結果情報を取得したか？
S43
NO
YES
認証結果を表示する
S44
エンド

【図１１】

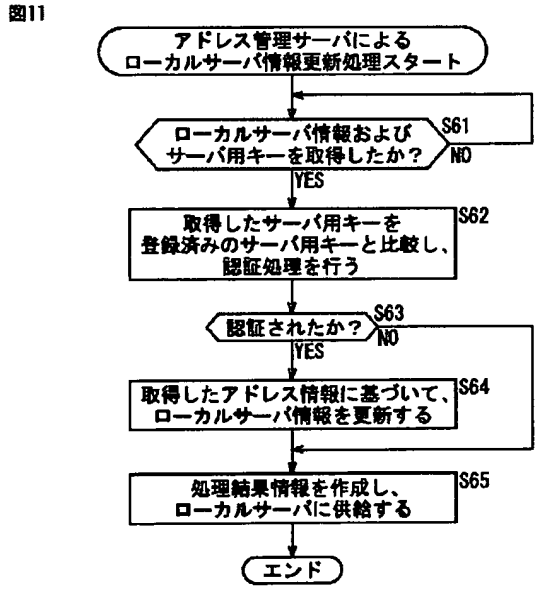
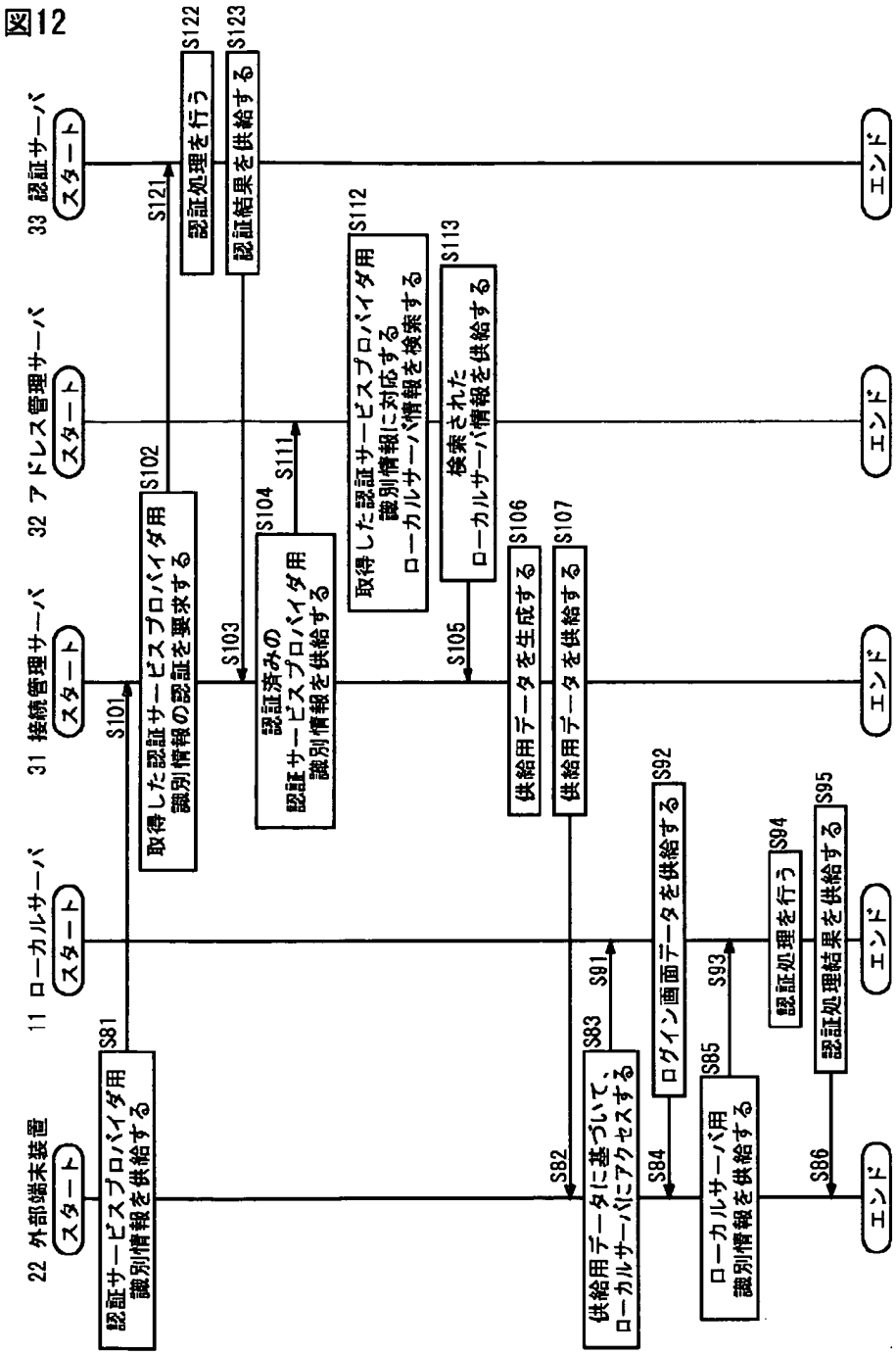


図11
アドレス管理サーバによる
ローカルサーバ情報更新処理スタート
ローカルサーバ情報および
サーバ用キーを取得したか？
S61
NO
YES
取得したサーバ用キーを
登録済みのサーバ用キーと比較し、
認証処理を行う
S62
認証されたか？
S63
NO
YES
取得したアドレス情報に基づいて、
ローカルサーバ情報を更新する
S64
処理結果情報を作成し、
ローカルサーバに供給する
S65
エンド

【図１２】

図12


22 外部端末装置
11 ローカルサーバ
31 接続管理サーバ
32 アドレス管理サーバ
33 認証サーバ
スタート
エンド
認証サービスプロバイダ用識別情報を供給する
S81
取得した認証サービスプロバイダ用識別情報の認証を要求する
S101
S102
認証処理を行う
S121
S122
認証結果を供給する
S123
S103
認証済みの認証サービスプロバイダ用識別情報を供給する
S104
S111
取得した認証サービスプロバイダ用識別情報に対応するローカルサーバ情報を検索する
S112
検索されたローカルサーバ情報を供給する
S113
S105
供給用データを生成する
S106
供給用データを供給する
S107
S82
供給用データに基づいて、ローカルサーバにアクセスする
S83
S91
ログイン画面データを供給する
S92
S84
ローカルサーバ用識別情報を供給する
S85
S93
認証処理を行う
S94
認証処理結果を供給する
S95
S86

【図１３】

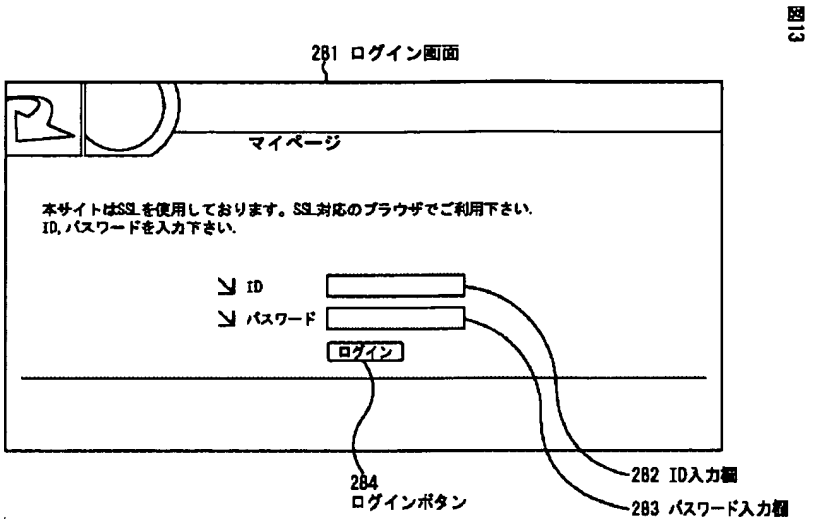


図13
281 ログイン画面
マイページ
本サイトはSSLを使用しております。SSL対応のブラウザでご利用下さい。
ID,パスワードを入力下さい。
ID
パスワード
ログイン
284
ログインボタン
282 ID入力欄
283 パスワード入力欄

【図１４】

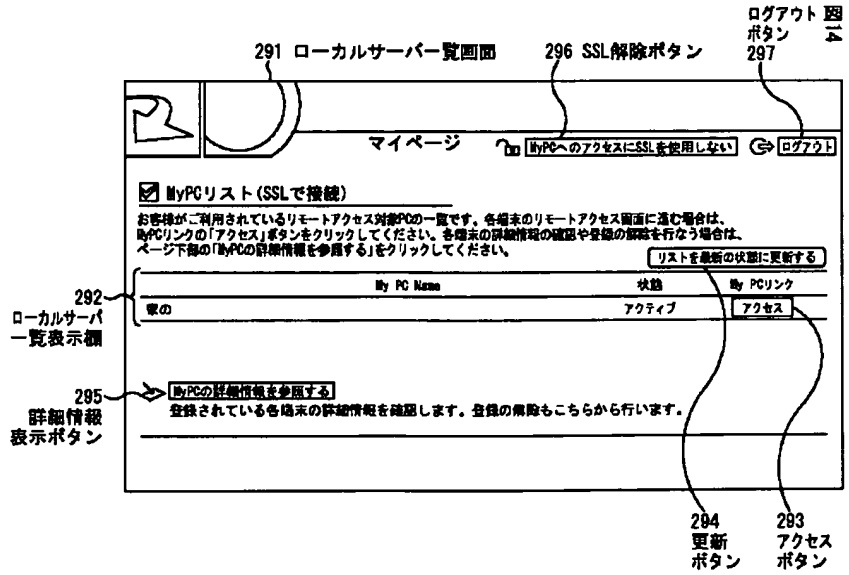
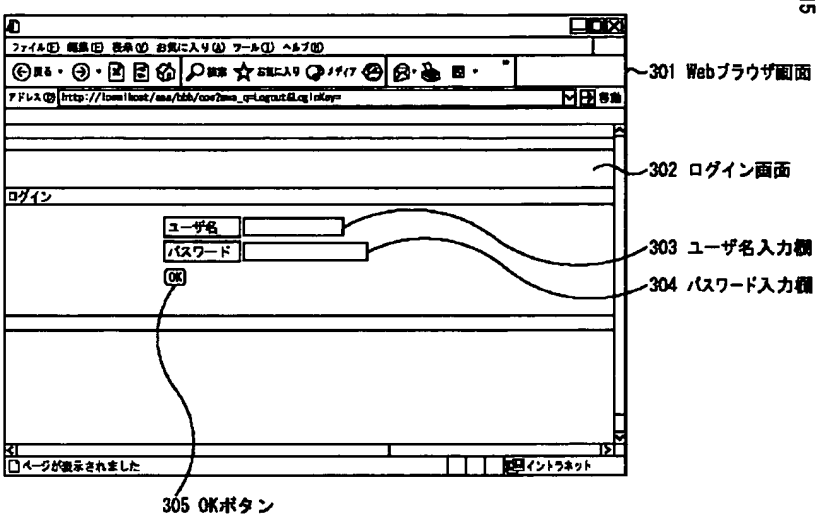


図14
ログアウト
ボタン
297
291 ローカルサーバー覧画面
296 SSL解除ボタン
マイページ
MyPCへのアクセスにSSLを使用しない
ログアウト
MyPCリスト(SSLで接続)
お客様がご利用されているリモートアクセス対象PCの一覧です。各端末のリモートアクセス画面に進む場合は、
MyPCリンクの「アクセス」ボタンをクリックしてください。各端末の詳細情報の確認や登録の解除を行なう場合は、
ページ下部の「MyPCの詳細情報を参照する」をクリックしてください。
リストを最新の状態に更新する
My PC Name
状態
My PCリンク
家の
アクティブ
アクセス
292
ローカルサーバ
一覧表示欄
295
詳細情報
表示ボタン
MyPCの詳細情報を参照する
登録されている各端末の詳細情報を確認します。登録の削除もこちらから行います。
294
更新
ボタン
293
アクセス
ボタン

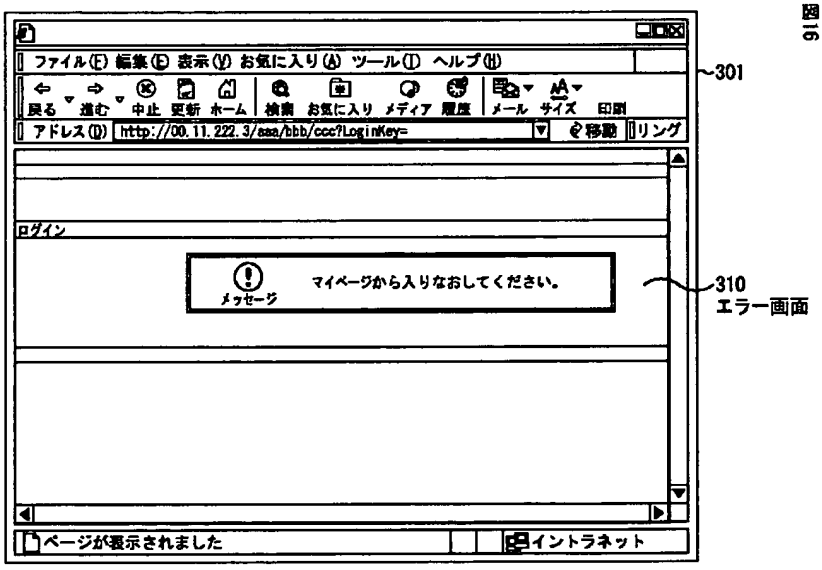
【図１５】

図15



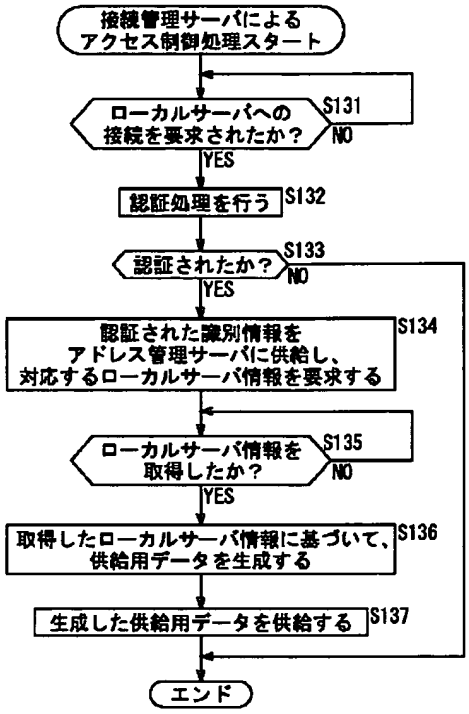
【図１６】

図16

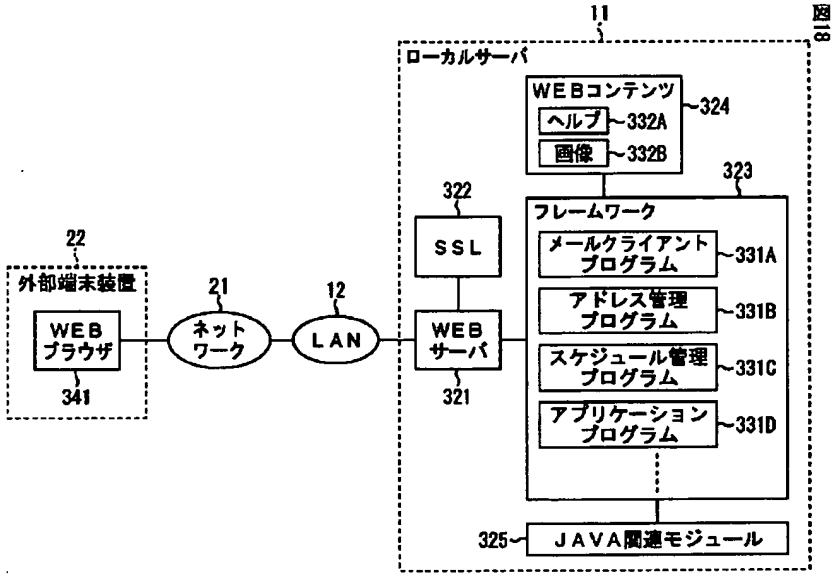


【図１７】

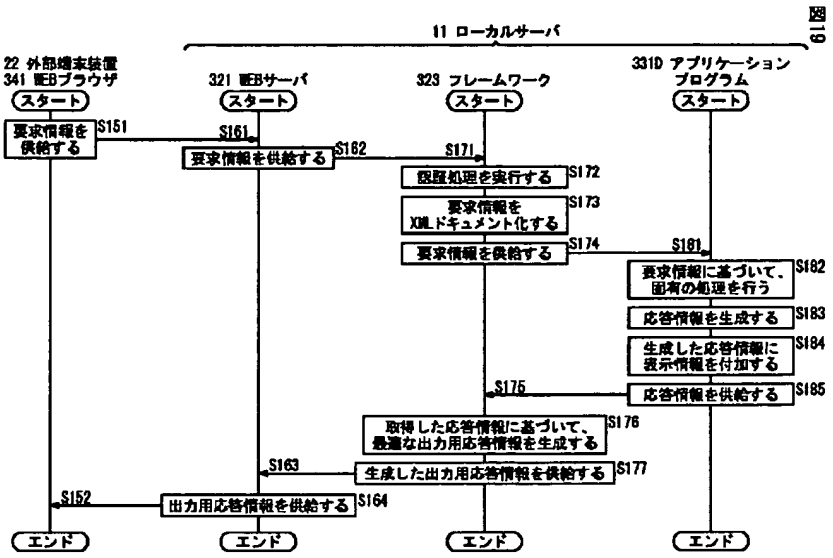
図17


接続管理サーバによる
アクセス制御処理スタート
ローカルサーバへの
接続を要求されたか？
S131
NO
YES
認証処理を行う
S132
認証されたか？
S133
NO
YES
認証された識別情報を
アドレス管理サーバに供給し、
対応するローカルサーバ情報を要求する
S134
ローカルサーバ情報を
取得したか？
S135
NO
YES
取得したローカルサーバ情報に基づいて、
供給用データを生成する
S136
生成した供給用データを供給する
S137
エンド

【図１８】


11
図18
ローカルサーバ
WEBコンテンツ
ヘルプ
332A
画像
332B
324
323
322
フレームワーク
SSL
メールクライアント
プログラム
331A
アドレス管理
プログラム
331B
スケジュール管理
プログラム
331C
アプリケーション
プログラム
331D
WEB
サーバ
321
325
JAVA関連モジュール
22
外部端末装置
WEB
ブラウザ
341
21
ネット
ワーク
12
LAN

【図１９】



【図２０】

図20

```
<?xml version="1.0" enooding="UTF-8"?>
<app>
 <_header cache-control="max-stale=0" host= "11.22.33.44:500" user-agent= "XXXXX/1.0/S000i/c10" />
 <_device media="chtml" maker= "XXXXX" version="1.0" name= "S000i" cache="10" un_ssllink="true" />
 <_request url="/xxx/yyy/zzz;jsessionid=yapu3corh1" sessionid=";jsessionid=yapu3corh1" method="GET"
remote_addr= "xxx.x.x.x" remote_host= "xxx.x.x.x" class= "xx/xx/xxxx" />
 <_dir user="D:/SSSS/xxx/zzz/demo" conf="D:/ SSSS/xxx/zzz/conf" web="D:/ SSSS/xxx/zzz/web/otml" />
 <_input q="View" id="1011067307834" />
 <_user ID="demo" Password="demo" LoginKey="testkey" />
 <_help url= "help.html" />
 <_message display="false" />
 <_output xsl= "output.xsl" />
 <_redirect send="false" uri ="/xxx/yyy/zzz;jsessionid=yapu3corh1" />
</app>
```

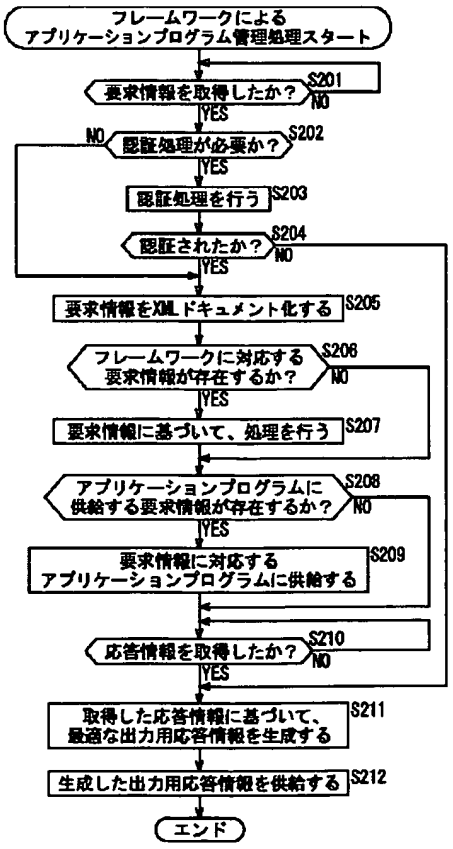
【図２１】

図21

```
<?xml version="1.0" encoding="UTF-8"?>
<app>
 <_header cache-control="max-stale=0" host= "11.22.33.44:500" user-agent= "XXXXXX/1.0/S000i/c10" />
 <_device media="chtml" maker= "XXXXXX" version="1.0" name= "S000i" cache="10" un_esllink="true" />
 <_request uri="/xxx/yyy/zzz;jsessionid=yapu3corh1" sessionid=";jsessionid=yapu3corh1" method="GET"
remote_addr= "xxx.x.x.x" remote_host= "xxx.x.x.x" class= "xx/xx/xxxx" />
 <_dir user="D:/SSSS/xxx/zzz/demo" conf="D:/ SSSS/xxx/zzz/conf" web="D:/ SSSS/xxx/zzz/web/ctml" />
 <_input q="View" id="1011087307834" />
 <_user ID="demo" Password="demo" LoginKey="testkey" />
 <_help url= "help_aaa.html" />
 <_message display= "true">
   <line id= "MSG-1" />
 </_message>
 <_output xsl= "output_aaa.xsl" />
 <_redirect send="false" uri ="/xxx/yyy/zzz;jsessionid=yapu3corh1" />
 <menu>
  <folderlist>
      .
      .
      .
 </menu>
</app>
```

【図２２】

図22



【図２３】

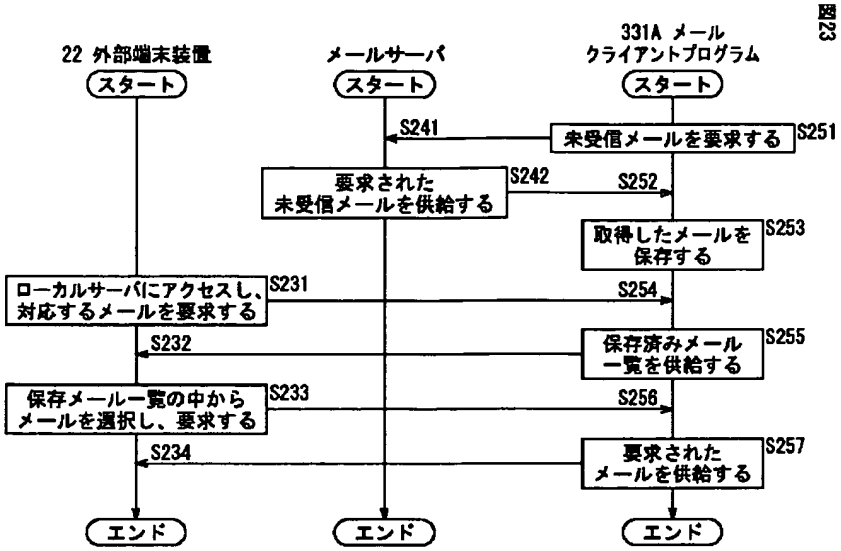


図23
22 外部端末装置
メールサーバ
331A メール
クライアントプログラム
スタート
スタート
スタート
S241
未受信メールを要求する
S251
要求された
未受信メールを供給する
S242
S252
取得したメールを
保存する
S253
ローカルサーバにアクセスし、
対応するメールを要求する
S231
S254
S232
保存済みメール
一覧を供給する
S255
保存メール一覧の中から
メールを選択し、要求する
S233
S256
S234
要求された
メールを供給する
S257
エンド
エンド
エンド

【図２４】

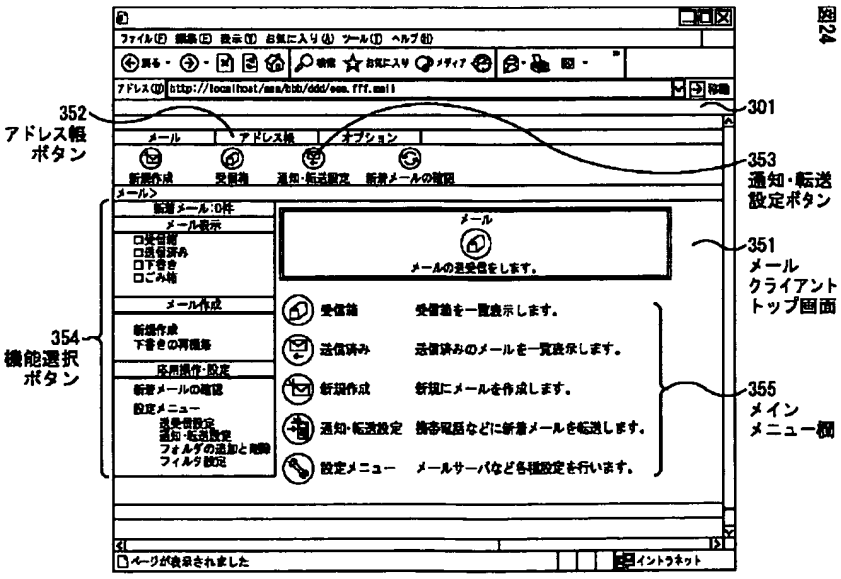
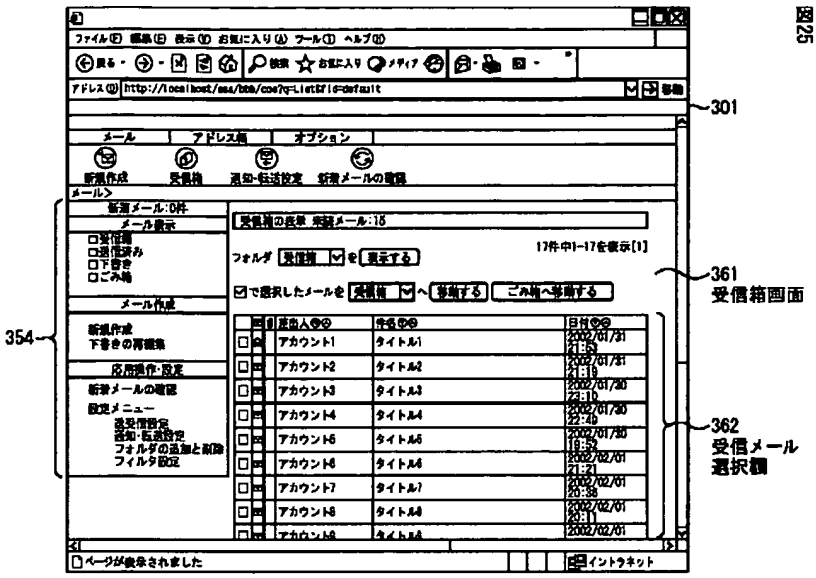
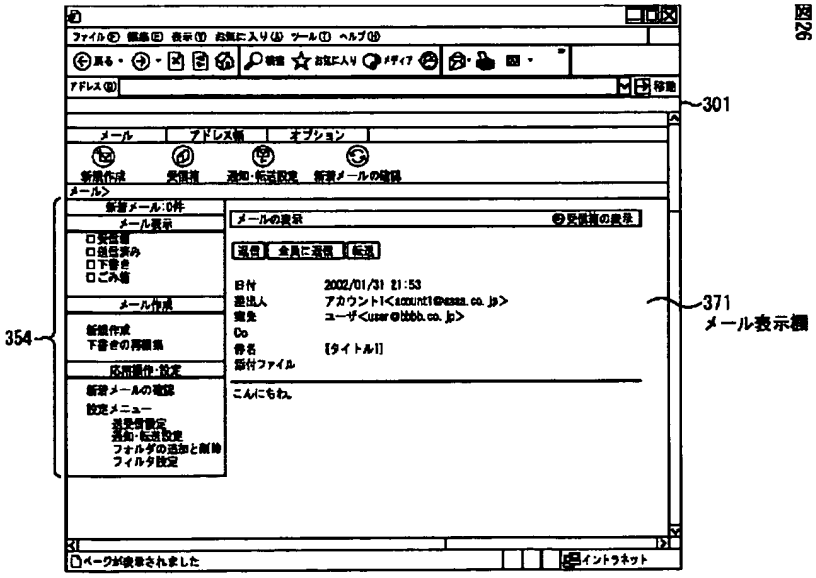


図24
352
アドレス帳
ボタン
301
353
通知・転送
設定ボタン
351
メール
クライアント
トップ画面
354
機能選択
ボタン
355
メイン
メニュー欄
メール
アドレス帳
オプション
新規作成
受信箱
通知・転送設定
新着メールの確認
メール
メールの送受信をします。
受信箱
受信箱を一覧表示します。
送信済み
送信済みのメールを一覧表示します。
新規作成
新規にメールを作成します。
通知・転送設定
携帯電話などに新着メールを転送します。
設定メニュー
メールサーバなどを各種設定を行います。

【図２５】



【図２６】



【図２７】

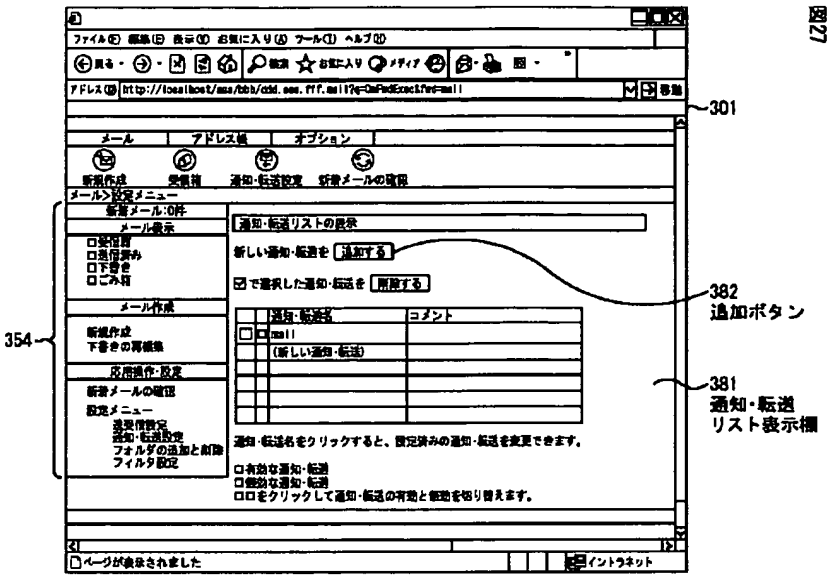


図27
301
354
382
追加ボタン
381
通知・転送
リスト表示欄

【図２８】

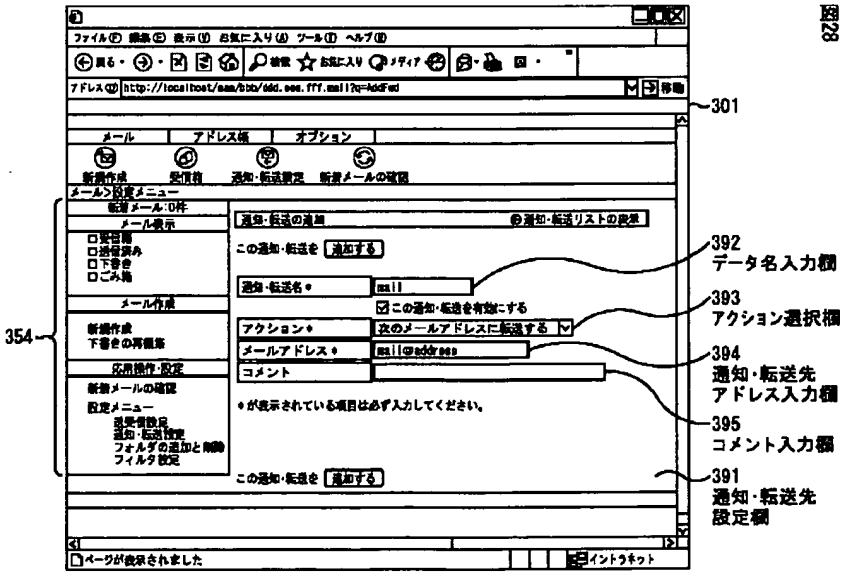
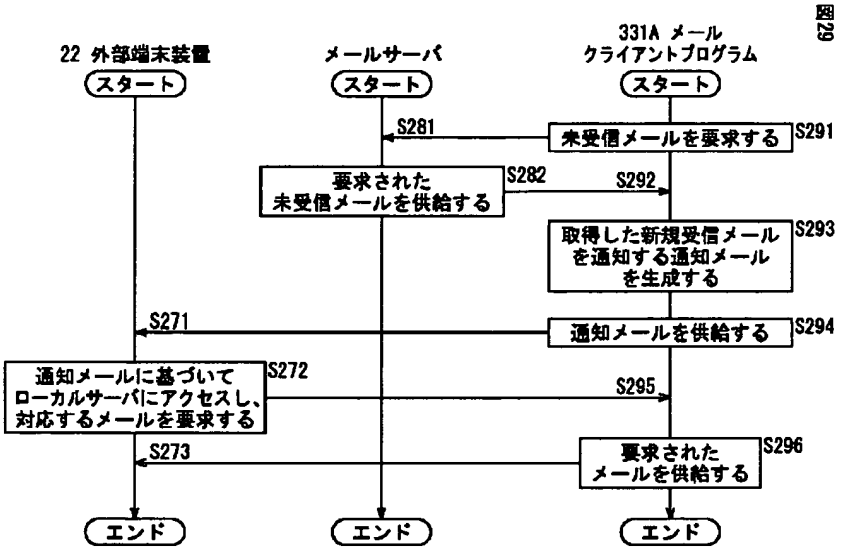
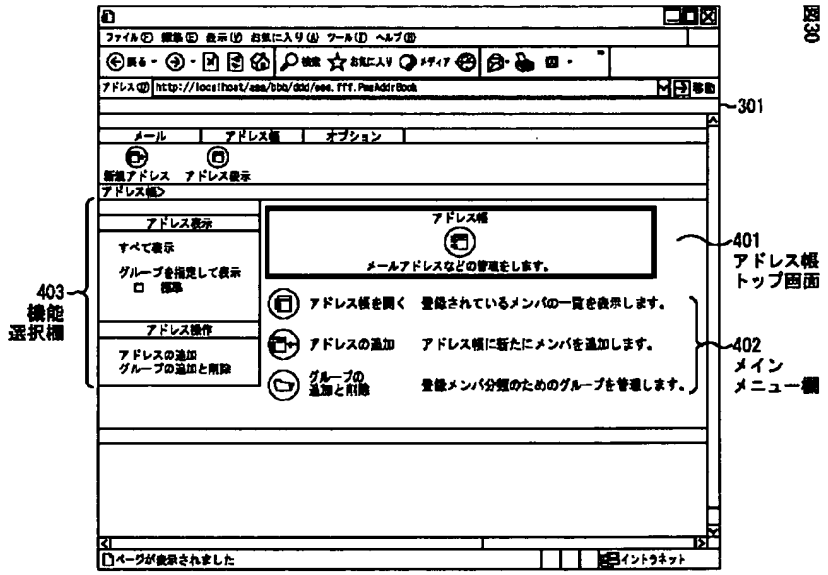


図28
301
354
392
データ名入力欄
393
アクション選択欄
394
通知・転送先
アドレス入力欄
395
コメント入力欄
391
通知・転送先
設定欄

【図２９】



【図３０】



フロントページの続き

(72)発明者　東原　正和
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　西浦　健一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　遠藤　悦伸
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B085 AE04 BC00